Kummer's criterion over Λ and Hida's Congruence Module

J. Tilouine

Series #4. August 1987

HOKKAIDO UNIVERSITY
TECHNICAL REPORT SERIES IN MATHEMATICS

#	Author	Title

1. T. Morimoto, Equivalence Problems of the Geometric Structures admitting Differential Filtrations
2. J. L. Heitsch, The Lefschetz Theorem for Foliated Manifolds
3. Twelfth Sapporo Symposium on Partial Differential Equations in 1987, Edited by K. Kubota

Kummer's criterion over Λ and Hida's Congruence Module.

J. Tilouine.

Acknowledgments.

These notes grew out of a series of lectures given at Hokkaido University, Sapporo, in June 1987 . This is my pleasure to thank profs. Doi K. and Hida H. to have made possible this stay in Sapporo, and also the J.S.P.S. to have supported it financially.

1. Introduction.

The purpose of these notes is to explain how one can use Hida's theory of ordinary Hecke algebra and of Congruence Module in order to obtain some information on(some part of)the Iwasawa module of the anticyclotomic $\mathbb{Z}_p$-extension of an imaginary quadratic field.

To be a little more precise, let K be a number field, p a rational prime number. We denote by S_p the set of primes in K above p , and take S to be any subset of S_p. Consider any $\mathbb{Z}_p$-extension K_∞/K and denote by M_∞^S the maximal abelian p-extension of K_∞ unramified outside S. Set $X_\infty^S = \mathrm{Gal}(M_\infty^S/K_\infty)$. Choose a topological generator of $\mathrm{Gal}(K_\infty/K)$. By this, we determine an isomorphism between the completed group algebra $\mathbb{Z}_p[[\mathrm{Gal}(K_\infty/K)]]$ and the so-called Iwasawa algebra $\Lambda = \mathbb{Z}_p[[T]]$. It is easy to prove by using class-field theory that the Λ-module X_∞^S is finitely generated (the action of $\mathrm{Gal}(K_\infty/K)$ on X_∞^S is given as usual by conjugation); for this fact as well as many basic facts in Iwasawa's theory, see, besides Iwasawa's papers, [3], [17] and [36].

Now ,suppose further that X_∞^S is a torsion Λ-module (this

happens when S is small in S_p , but for $S=S_p$ itself, this is not true). Then we can speak of the characteristic power series of X_∞^S . The knowledge of this series provides some deep insight in the arithmetic of K_∞/K; thus it is very important to determine this series explicitly. Let us give a celebrated example of such a determination. Consider a totally real field F and let K be the field generated over F by a primitive p^{th}-root of unity ζ_p. We write Δ for the Galois group of K/F. The Teichmüller character $\omega:\Delta \longrightarrow \mathbb{F}_p^x$ generates the dual group of Δ. We call it the basic cyclotomic character. Now , we look at the cyclotomic $\mathbb{Z}_p$-extension , whose n^{th} layer K_n is defined to be $F(\zeta_{p^{n+e}})$, where ζ_{p^r} denotes a primitive $(p^r)^{th}$ root of unity and e is the largest integer such that $\zeta_{p^e} \in K$, whence $[K_n:K]=p^n$. We choose S to be the empty set ϕ, then it is easy to check that X_∞^ϕ is Λ-torsion. We may canonically lift ω to $\mathbb{Z}_p^x$ .We still denote it by ω but we understand that it takes values in the ring $\mathbb{Z}_p$ of characteristic 0. Furthermore , for each integer i mod.p-1, we consider the ω^i-part of X_∞^ϕ for the action of Δ, denoted by $X_\infty^\phi(\omega^i)$. When $F=\mathbb{Q}$, the Vandiver conjecture predicts that for all even such i's the corresponding component $X_\infty^\phi(\omega^i)$ is trivial, and Herbrand theorem shows that for $i\equiv 1$ mod.p-1, the corresponding component is also trivial (see [17] chap.3 and [36] §6.3); we therefore restrict ourselves to odd i's , $\not\equiv 1$ mod.p-1. Let $f_i(T)\in\Lambda$ be the characteristic power series of $X_\infty^\phi(\omega^i)$ for such i's.

On the other hand , Kubota and Leopoldt ([14], in the

case $F=\mathbb{Q}$) and Deligne-Ribet ([26],[29],for an arbitrary totally real field F, see also Th.4.4 of [8]) have constructed for each such integer i mod.p-1(i.e.odd and $\not\equiv 1$ mod.p-1) a power series $g_i(T)\in\Lambda$ interpolating the special values of the zeta function of F, twisted by the character ω^{1-i}; namely:

$$g_i((1+p)^s-1)= L_p(-s,\omega^{1-i}) \quad , \quad \text{for all } s \text{ in } \mathbb{Z}_p \ ,$$

where the p-adic L function L_p satisfies for all integer k such that $k\equiv i$ mod.p-1 :

$$L_p(1-k,\omega^{1-i})= L(1-k,\omega^{1-i}) \ .$$

Now , the theorem of Mazur-Wiles [21](for $F=\mathbb{Q}$) and of Wiles (for any totally real F, now in print in Inv. Math.) asserts that, up to a unit in Λ, the power series $f_i(T)$ and $g_i(T)$ coincide.

In this text , we want to deal with the following situation of the imaginary case which is parallel to the totally real case.

Let M be an imaginary quadratic field, p a rational prime number which splits in M, say $(p)=p.p^{\rho}$, where ρ is the complex conjugation in M. Our ground field for the Iwasawa theory is now K=M(p) which is the Ringklassenkörper of the order of conductor p in M. We still write Δ for the Galois group of K/M. For simplicity, let us suppose in this introduction that the class number of M is one. Then, we have a basic anticyclotomic character κ: $\Delta \to \mathbb{F}_p^x$ which generates the dual group of Δ (see §4 for its definition). We consider, instead of the cyclotomic $\mathbb{Z}_p$-extension of K, the anticyclotomic one, whose n^{th} layer is defined to be $K_n= M(p^{n+1})$, the Ring -

klassenkörper of the order of conductor p^{n+1} in M. The $\mathbb{Z}_p$-extension K_∞/K is called anticyclotomic because K_∞ is Galois over $\mathbb{Q}$ but the action of ρ on $Gal(K_\infty/K)$ by conjugation is by inversion : $\sigma \to \sigma^{-1}$, instead of being trivial (as it is in the cyclotomic case). We take the set of primes in K above p as subset S of S_p ; it means that we take only half of S_p. In this case, one can show (cf.§4) that X_∞^S is torsion over the Iwasawa algebra Λ (identified as previously to the completed group algebra of $Gal(K_\infty/K)$). Recall that the number of units in M is 2e. Here, usually e=1. But there are two exceptional cases; i.e. e=2 when $M=\mathbb{Q}(\sqrt{-1})$ and e=3 when $M=\mathbb{Q}(\sqrt{-3})$. We consider any integer i mod.p-1 such that $ei \not\equiv 0,1$ mod.p-1 and we look at the κ^i-part of X_∞^S , say $X_\infty^S(\kappa^i)$, for the action of Δ. Let $f_i(T)$ be its characteristic power series in Λ.

Now, Hida's theory [10] allows us to define a Congruence Module attached to M and i (as will be explained in §1 and 2) which is a Λ-module much easier to handle; namely , it is isomorphic to $\Lambda/(H_i)$ for some suitable element $H_i(T)$ in Λ.

Now , our aim is to show the link between the Iwasawa module $X_\infty^S(\kappa^i)$ and the Congruence Module ; this link implies in particular that $H_i(T)$ divides (twisted) $f_i(T)$ in Λ . This is the main theorem in these notes (th.4.3 below). Note that it is conjectured that $H_i(T)$ coincides with the specialisation to the anticyclotomic variable of the Katz-Yager p-adic L function of two variables corresponding to the branch κ^i (in the Yager's terminology, it corresponds to the pair (i,-i)).

Therefore, according to the Main Conjecture of Iwasawa-Coates

(presented in [3]), it is believed that those three power series coincide, up to a unit in Λ. We hope to prove partial results in this direction in a subsequent paper.

Let us add that the idea of comparing the values at T=0 of $H_i(T)$ and (twisted) $f_i(T)$ was already present in [9] which is the origin of our work.

Contents

0. Introduction 3

1. Hida's theory of the ordinary Hecke algebra and of the Congruence Module 8

2. Component of h^{ord} of C.M. type attached to a Grössencharacter of an imaginary quadratic field 24

3. Gorenstein-ness of the local component associated to a Grössencharacter 32

4. The anticyclotomic $\mathbb{Z}_p$-extension and its Iwasawa theory 45

5. The Λ-divisible group attached to the local component and the Λ-linear map from (twisted) $X_\infty^S(\kappa^i)$ to the module of differentials 54

6. The properties of the map a_∞ 66

7. Surjectivity of a_∞ 72

8. An exact sequence for the Congruence Module and module of differentials 74

9. A link between the Fitting ideals of C_0 and C_1 78

1. Hida's theory of ordinary Hecke algebra and the Congruence Module

The reference for the unproved theorems of this paragraph is mainly [10] where Hida first developed his " control theory " of the ordinary Hecke algebra and also [39] for the modified version using a finite normal extension of the Iwasawa algebra as base ring instead of Λ.

Let N be an integer >0 and p be a fixed odd prime which doesn't divide N . We will be concerned chiefly with the following congruence subgroups :

$$\Gamma_1(Np^r)=\{\begin{pmatrix} a & b \\ c & d \end{pmatrix}\in SL_2(\mathbb{Z}) ; c\equiv 0 \mod .Np^r,\ a\equiv d\equiv 1 \mod .Np^r\}$$

where r is any positive integer.

For each integer $k>0$, let $S_k(\Gamma_1(Np^r))$ be the $\mathbb{C}$-vector space of parabolic modular forms of weight k for the congruence subgroup $\Gamma_1(Np^r)$. By taking the Fourier expansion of those forms we obtain a $\mathbb{C}$-linear embedding :

$$S_k(\Gamma_1(Np^r)) \to \mathbb{C}[[q]] ,$$

$$f=\sum_{n=0}^{\infty} a(n,f)\exp(2\pi inz) \to \sum_{n=0}^{\infty} a(n,f)q^n$$

So, in particular, we can set for any subring A of $\mathbb{C}$:

$$S_{k,r}(A) = S_k(\Gamma_1(Np^r)) \cap A[[q]]$$

Furthermore, for any integer a prime to Np, let $\sigma_a \in SL_2(\mathbb{Z})$ be any matrix congruent to $\begin{pmatrix} a^{-1} & \\ & a \end{pmatrix}$ mod.Np^r. It acts on $S_k(\Gamma_1(Np^r))$ by the action of weight k (cf.[32] chapter 3 ,§4)

This gives a representation, called diamond of weight k :

$$\langle\ \rangle_k : (\mathbb{Z}/Np^r\mathbb{Z})^x \to \mathrm{Aut}(S_{k,r}(\mathbb{C}))\ ,\ \text{whose kernel is } \{\pm 1\}.$$

This map can also be viewed as the identification of $(\mathbb{Z}/Np^r\mathbb{Z})^x$ with $\Gamma_0(Np^r)/\Gamma_1(Np^r)$ acting in weight k.

Then, one can recall the definition of Hecke operators as endomorphisms of $S_{k,r}(\mathbb{C})$. For any n>0 , we set :

$$f|T(n) = n^{\frac{k}{2}-1} \cdot \sum_{\substack{a>0 \\ (a,N)=1,\, ad=n \\ b \bmod d}} f|_k \sigma_a \begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$$

We denote for each subring A of $\mathbb{C}$ by $h_{k,r}(A)$ the A-subalgebra of $\mathrm{End}(S_{k,r}(\mathbb{C}))$ generated by all the T(n)'s. It is well known that the pairing

$$(1.1) \qquad h_{k,r}(\mathbb{C}) \times S_{k,r}(\mathbb{C}) \to \mathbb{C}$$
$$(T\ ,\ f) \longmapsto a(1, f|T)$$

is perfect (see for instance [32] Theo.3.45).

We want to use all those notions and results for $S_{k,r}(A)$, A being any ring in place of $\mathbb{C}$. For this, we first check the compatibility for the extension of scalars.

Lemma 1.1: Suppose that k>1. For any subring A of $\mathbb{C}$, the canonical homomorphisms:

$$S_{k,r}(\mathbb{Z}) \otimes A \to S_{k,r}(A) \quad \text{and} \quad h_{k,r}(\mathbb{Z}) \otimes A \to h_{k,r}(A)$$

are isomorphisms.

Proof: We abbreviate $h_{k,r}(A)$ (resp.$S_{k,r}(A)$) by h(A) (resp.S(A)). Recall that according to Theorem 8.4 and Prop.8.6 of [32] ,

there exists a lattice L in $S(\mathbb{C})$ stable under $h(\mathbb{Z})$. We therefore have a faithful representation $h(\mathbb{Z}) \to \mathrm{End}_{\mathbb{Z}}(L)$. Let κ be the dimension of $S(\mathbb{C})$. If we fix a basis of L over $\mathbb{Z}$, we get a matricial representation :

(1) $\quad \Omega : h(\mathbb{Z}) \to M_{2\kappa}(\mathbb{Z})$

Set $\Omega(n)=(\omega_{i,j}(n))_{i,j}$ and let us introduce the series

$$f_{i,j} = \sum_{n>0}^{\infty} \omega_{i,j}(n).q^n$$

By the definition of Ω, we see that $f_{i,j} \in S(\mathbb{Z})$. Besides, the $f_{i,j}$'s generate $S(\mathbb{C})$. To check this, take any f in $S(\mathbb{C})$. It defines a linear form $\lambda_f : h(\mathbb{Z}) \to \mathbb{C}$. As $\mathbb{C}$ is divisible, we can define $\tilde{\lambda}_f : M_{2\kappa}(\mathbb{Z}) \to \mathbb{C}$ such that $\tilde{\lambda}_f \circ \Omega = \lambda_f$.

Let $\pi_{i,j} : M_{2\kappa}(\mathbb{Z}) \to \mathbb{Z}$, $(a_{\alpha,\beta}) \longmapsto a_{i,j}$ be the canonical linear forms on $M_{2\kappa}(\mathbb{Z})$. We can write

$\tilde{\lambda}_f = \sum_{i,j} c_{i,j}\, \pi_{i,j}$ for some complex numbers $c_{i,j}$'s.

Thus, for each $n>0$, we have :

$a(n,f) = \sum_{i,j} c_{i,j}\, \omega_{i,j}(n)$, and finally, $f = \sum_{i,j} c_{i,j}\, f_{i,j}$.

Besides, it is obvious that the map $S(\mathbb{Z}) \otimes \mathbb{C} \to S(\mathbb{C})$ is injective, so it is bijective.

Now, let us show that $S(\mathbb{Z})$ is free of rank κ over $\mathbb{Z}$. We deduce from (1) that $h(\mathbb{Z})$ is a finite free $\mathbb{Z}$-algebra. Let $(T(n_i))_{i=1,..,s}$ a subset of $\{T(n)\}_{n>0}$ which generates the module $\sum_{n>0} \mathbb{Z}.T(n)$ over $\mathbb{Z}$. Then :

$$S(\mathbb{Z}) = \{f \in S(\mathbb{C}) \ ; \text{ for } i=1,\ldots,s \ , a(n_i,f) \in \mathbb{Z}\}$$

so that we have a linear injection with torsion-free cokernel:

$$\varphi : S(\mathbb{Z}) \to \mathbb{Z}^s \ , \ f \longmapsto (a(n_i,f))_{i=1,\ldots,s}$$

From this, we first see that $S(\mathbb{Z})$ is free (obviously of rank

κ). Secondly, if A is any subring of $\mathbb{C}$, if we denote by φ_A the extension of scalars of φ to A, we see by flatness of the cokernel of φ that :

$$\text{Im } \varphi_A = (\text{Im } \varphi_{\mathbb{C}}) \cap A^S$$

so that $S(\mathbb{Z}) \otimes A \cong S(A)$.

Now, for each subring A of $\mathbb{C}$, consider the obvious A-algebra morphism :

(2) $\quad h(\mathbb{Z}) \otimes A \longrightarrow h(A)$

By the perfectness of the pairing (1.1), we know that dim $h(\mathbb{C})$ equals κ. Then, to prove that the rank of $h(\mathbb{Z})$ is κ, we notice that the natural morphism:

(3) $\quad h(\mathbb{R}) \otimes \mathbb{C} \longrightarrow h(\mathbb{C})$

is an isomorphism . In fact, the antilinear automorphism

$K: f(z) \mapsto \overline{f(-\bar{z})}$ of $S(\mathbb{C})$ acts by conjugation on $h(\mathbb{C})$, so, if T_1 and T_2 are elements of $h(\mathbb{R})$ such that $T_1 + iT_2 = 0$, we have $(T_1+iT_2)^K = T_1 - iT_2 = 0$, hence $T_1 = T_2 = 0$. But, on the other hand, we have $S(\mathbb{C}) = L \otimes \mathbb{R}$, hence $\text{End}_{\mathbb{R}}(S(\mathbb{C})) = (\text{End}_{\mathbb{Z}} L) \otimes \mathbb{R}$; this yields the injectivity of $h(\mathbb{Z}) \otimes \mathbb{R} \longrightarrow h(\mathbb{R})$, i.e. the rank of $h(\mathbb{R})$ is κ. We conclude now to the injectivity of (2) for $A = \mathbb{C}$ because of the remark (3) above, and finally for every subring A of $\mathbb{C}$. Q.E.D.

Now, we can extend the notations for any ring A :

$$S(A) = S_{k,r}(A) = S_{k,r}(\mathbb{Z}) \otimes A \ , \quad h(A) = h_{k,r}(A) = h_{k,r}(\mathbb{Z}) \otimes A \ .$$

If we handled with $\Gamma_0(Np^r)$ instead of $\Gamma_1(Np^r)$, it would be obvious that the analogous Hecke algebra $h(\mathbb{Z})$ leaves stable the analogous $S(\mathbb{Z})$, hence, that we could define a natural

representation $h(A) \to End_A S(A)$. But in the case of $\Gamma_1(Np^r)$, the difficulty comes from the diamonds automorphisms (which don't exist for Γ_0). Still, it is true that our $h(\mathbb{Z})$ leaves $S(\mathbb{Z})$ stable but the proof of this fact requires Katz's theory of p-adic modular forms. It can be found in [10], §1. We will take this for granted in the following. It allows us to look at $h(A)$ as a subalgebra of $End_A S(A)$ when A has no torsion as abelian group . Call this hypothesis (flat.).

Lemma 1.2: Assuming (flat.) ,the A-linear pairing :

$$h(A) \times S(A) \to A \ , \ (T,f) \mapsto a(1,f|T)$$

is perfect.

Proof:We can suppose $A=\mathbb{Z}$. Since we proved that $S(\mathbb{Z})$ is free of rank $\kappa=\dim_{\mathbb{C}} S(\mathbb{C})$, the result is obvious by perfectness of (1.1).

Remark: In order to check that $S(\mathbb{Z})$ is stable under $h(\mathbb{Z})$, we may check it locally . This is very easy for all prime numbers outside $\varphi(M)$(where $M=Np^r$is the level of $\Gamma_1(M)$). Just extend the scalars to $\mathbb{Z}_{(q)}[\zeta_M]$ (q is a fixed prime number outside $\varphi(M)$, and ζ_M is a primitive M^{th}root of unity). We can now use the idempotents of the group algebra $\mathbb{Z}_{(q)}[\zeta_M][(\mathbb{Z}/M\mathbb{Z})^x]$ to decompose the action of the diamonds on $S(\mathbb{Q}(\zeta_M))$ according to eigenspaces so that the stability of $S(\mathbb{Z}_{(q)}[\zeta_M])$ under the diamonds is obvious. But, to deal with the primes dividing $\varphi(M)$, no elementary mean is known to me.

After those preliminaries, we may introduce p-adic modular forms in Hida's version. The previous notations remain in use. For any couple (k,r), $k>0$, $r\geq 0$, we consider the inclusion given by q-expansion :

$$S_{k,r}(\mathbb{Z}) \longrightarrow \mathbb{Z}[[q]]$$

and tensor it by $\mathbb{Z}_p$ or $\mathbb{Q}_p$. It is easy to check that for any fixed $r \geq 0$, the following map is still injective:

$$\bigoplus_{k>0} S_{k,r}(\mathbb{Q}_p) \longrightarrow \mathbb{Q}_p[[q]]$$

[it is enough to check it for $\mathbb{Q}$ or even $\mathbb{C}$ instead of $\mathbb{Q}_p$. So, if $\sum_{k>0} f_k = 0$, we have also $\sum j(\gamma,z)^k f_k = 0$ for all γ in $\Gamma_1(Np^r)$, where $j\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}, z\right) = (cz+d)$. Then we use the cocycle formula $j(\gamma\gamma',z)=j(\gamma',z)\ j(\gamma,\gamma'z)$ to conclude the proof as Artin's lemma of independance of characters (or cocycles)].

Then, one defines :

$$S_{.,r} = \left(\bigoplus_{k>0} S_{k,r}(\mathbb{Q}_p)\right) \cap \mathbb{Z}_p[[q]]$$

Note that if $0 \leq r \leq r'$, we have obvious inclusions $S_{.,r} \subset S_{.,r'}$. Besides, there is a natural topology on $\mathbb{Q}_p[[q]]$ given by the norm $\left| \sum_{n \geq 0} \lambda_n q^n \right|_p = \sup_{n \geq 0} |\lambda_n|_p$. Let $\bar{S}_{.,r}$ be the closure of $S_{.,r}$ in $\mathbb{Z}_p[[q]]$. Then, by using Katz'theory of p-adic modular forms, Hida shows :

Theorem 1.3: For each $r' \geq r \geq 0$, the inclusion $\bar{S}_{.,r} \subset \bar{S}_{.,r'}$ is an equality. Furthermore ,if we denote by $\bar{S}$ the common value of these modules $\bar{S}_{.,r}$, the cokernel of the inclusion

$$\bar{S} \longrightarrow \mathbb{Z}_p[[q]]$$

is a torsion free $\mathbb{Z}_p$-module.

Proof: See [10],§1. The last assertion is Katz's p-adic q-expansion principle. It can be deduced (cf.[15])from the irreducibility of the modular scheme (proved in [26]).

Corollary 1.4 : For each $r \geq 0$, each $k>0$, $S_{k,r}(\mathbb{Z}_p) \subset \bar{S}$.

After defining the space of p-adic modular forms , we define the big Hecke algebra which acts on it. Take $r \geq 0$, and remark that $\mathrm{End}_{\mathbb{Z}_p}(S_{.,r}) = \mathrm{End}_{\mathbb{Z}_p}(\bar{S})$. First ,it is also a consequence of Katz's theory that, defining for any integer n an operator T(n) on $\oplus_{k>0} S_{k,r}(\mathbb{Q}_p)$ by: $(\sum_{k>0} f_k)|T(n) = \sum_{k>0} f_k|T(n)$, the submodule $S_{.,r}$ is stable for T(n). It is obvious that for $0<r\leq r'$, this action is compatible with the inclusion $S_{.,r} \subset S_{.,r'}$; so, if we introduce the closed subalgebra h_r of End $S_{.,r}$ generated by the T(n)'s, it is clear that it doesn't depend on r. We denote it by h and we call it the big Hecke algebra. For the details concerning the use of Katz's theory to define h, see §1 of [10] and [15].

Let us now define the ordinary part of Hecke algebras. Let T(p) be the p^{th} Hecke operator acting on $\bar{S}$. We have $T(p) \in h$. By looking at its definition, it is not difficult to see that h is a profinite $\mathbb{Z}_p$-algebra. From this, it results that h can be decomposed as a product of two algebras :

$$(1.4) \qquad h \cong h^{ord} \times h^{s.s.}$$

where h^{ord} (ordinary part) is the biggest quotient (or sub-) algebra on which T(p) is invertible, and $h^{s.s.}$ (supersingular part) the biggest quotient (or sub-) algebra on which T(p) is topologically nilpotent. In fact, we can write $h = \varprojlim h_i$ where h_i is an artinian $\mathbb{Z}_p$-algebra, so we can use the structure theorem for artinian rings:

h_i is a product of local Artin rings

we take : h_i^{ord} = product of those local components in which

T(p) is invertible.

$h_i^{s.s.}$ = product of those local components in which T(p) belongs to the maximal ideal (i.e. is nilpotent).

This decomposition is compatible with the transition morphisms and gives (1.4) at the limit.

Let e be the unit element of h^{ord}. We call e the ordinary idempotent of h. Similarly, we get decomposition of all Hecke algebras $h_{k,r} = h_{k,r}(\mathbb{Z}_p)$ as product of $h_{k,r}^{ord}$ and $h_{k,r}^{s.s.}$. Because of corollary 1.4, we have an obvious surjective morphism:

$$(1.5) \quad h \dashrightarrow h_{k,r} \quad , (k>0 \ , \ r>0).$$

It is clear that the idempotent e is mapped to the analogous idempotent $e_{k,r}$ of $h_{k,r}$. We define :

$$\bar{S}^{ord} = e.\bar{S} \ , \ S_{k,r}^{ord} = e.S_{k,r} = e_{k,r}.S_{k,r}.$$

Furthermore, by taking the inverse limit on r of the maps (1.5), we get a surjective homomorphism of $\mathbb{Z}_p$-algebras :

$$h \dashrightarrow \varprojlim_r h_{k,r}$$

This morphism is an isomorphism if and only if $\bigcup_{r>0} S_{k,r}(\mathbb{Z}_p)$ is dense in $\bar{S}$. A difficult theorem by Shimura and Ohta asserts that this is true, but we can avoid to use it if we concentrate ourselves on the ordinary parts (cf. [11] th.1.1).

Theorem 1.5: For each $k \geq 2$, the natural morphism of $\mathbb{Z}_p$-algebras

$$(1.5) \qquad h^{ord} \dashrightarrow \varprojlim_r h_{k,r}^{ord}$$

is an isomorphism.

This allows us to define a supplementary structure on h^{ord}: fix $k \geq 2$ and look at the diamond of weight k.

$\langle . \rangle_k : (\mathbb{Z}/Np^r\mathbb{Z})^x \dashrightarrow h_{k,r}$ (the image falls in the Hecke

algebra because we can write $\langle a\rangle_k = (T_\ell^2 - T_{\ell^2})/\ell^{k-1}$, ℓ being any prime such that $\ell \equiv a \bmod Np^r$, $\ell \neq p$).

Take the inverse limit of these compatible maps and take the ordinary part on the right. We get a homomorphism (whose kernel is ± 1): $\langle . \rangle_k : Z \to h^{ord}$, where $Z = \varprojlim_r (\mathbb{Z}/Np^r\mathbb{Z})^\times$.

We have the decompositions : $Z \simeq (\mathbb{Z}/N\mathbb{Z})^\times \times \mathbb{Z}_p^\times \simeq (\mathbb{Z}/N\mathbb{Z})^\times \times \mu_{p-1} \times \Gamma$,where $\Gamma = 1+p\mathbb{Z}_p$ is identified by this isomorphism to $\{z \in Z; z \equiv 1 \bmod. Np\}$ and μ_{p-1} is the group of $(p-1)^{st}$ roots of unity in $\mathbb{Z}_p^\times$ We choose $u=1+Np$ as topological generator of $\{z \in Z; z \equiv 1 \bmod. Np\}$.

Finally, to avoid the choice of a weight k, we introduce the diamonds of weight 0 : for $z=(z_N, z_p) \in Z = (\mathbb{Z}/N\mathbb{Z})^\times \times \mathbb{Z}_p^\times$, we set

(1.6) $\qquad \langle z\rangle_0 = z_p^k . \langle z\rangle_k$

Then, the map $\langle . \rangle_0 : Z \to h^{ord}$ gives a structure of $\mathbb{Z}_p[[Z]]$-module on h^{ord}. Via the inclusion $\mu_{p-1} \to Z$, we have an action of the group μ_{p-1} of order prime to p on the $\mathbb{Z}_p$-algebra h^{ord}; hence we may decompose it in eigenspaces $h^{ord}(a)$, $a \in (\mathbb{Z}/(p-1)\mathbb{Z}$ (dual of μ_{p-1}):

$$h^{ord}(a) = \{T \in h^{ord}; \langle \zeta\rangle_0 . T = \zeta^a . T \text{ for all } \zeta \text{ in } \mu_{p-1}\}$$

We consider h, h^{ord}, $h^{ord}(a)$ $(a \in (\mathbb{Z}/(p-1).\mathbb{Z})$ as algebras over the Iwasawa algebra $\Lambda = \mathbb{Z}_p[[T]]$ via:

(1.7) $\qquad \Lambda \to \mathbb{Z}_p[[Z]]$, $T \to \langle u\rangle_0 - 1$, $u = 1+Np$.

Remark: In order to deal with modular forms with coefficients in an arbitrary finite extension of $\mathbb{Q}_p$, say L, it is useful and easy to reformulate all the previous considerations with a base ring $\mathcal{O}_L$ instead of $\mathbb{Z}_p$ ($\mathcal{O}_L$ being the ring of integers in L) so, we have $\bar{S}(\mathcal{O}_L) = \bar{S} \otimes \mathcal{O}_L$, $h(\mathcal{O}_L) = h \otimes \mathcal{O}_L$, $h_{k,r}(\mathcal{O}_L) = h_{k,r} \otimes \mathcal{O}_L$

and so on; all the theorems of this paragraph hold *mutato mutandis* in this context. In particular, $h(\mathcal{O}_L)$ becomes a Λ_L-module; $\Lambda_L = \mathcal{O}_L[[T]]$. We will not make the obvious translations to this situation but take it for granted in the next paragraph. For details, see [10] §3.

We are now able to set the first important result of Hida's theory (proof:[10] Th.3.1).

Theorem 1.6: h^{ord} is a finite free Λ-module.

Commentary: In some sense, it means that diamonds automorphisms control all the ordinary Hecke algebra. This is the reason why this part of the Hecke algebra can be precisely studied. But it is conjectured that the whole Hecke algebra is finite over the Iwasawa algebra of four variables, so, the ordinary part is a very small part of the whole.

In addition to theorem 1.6, there are control theorems for the isomorphism (1.5). Perhaps, we should rather say that we have an Iwasawa theory for this isomorphism, since they will allow us to recover the projective system from the datum of the limit , as quotient by Iwasawa polynomials.

For $r>0$, $k>1$, set $\omega_{k,r}(T) = (1+T)^{p^{r-1}} - u^{k.p^{r-1}}$ (twisted Iwasawa polynomials). Note that $S_{k,r} \subset \bar{S}[\omega_{k,r}(T)]$, by which we mean the part of $\bar{S}$ killed by $\omega_{k,r}(T)$. Hence, we have a natural morphism :

$$(1.7) \qquad h^{ord}/\omega_{k,r}(T).h^{ord} \longrightarrow h^{ord}_{k,r} \ .$$

Theorem 1.7: If $k>1$, $r>0$, the map (1.7) is an isomorphism.

Remark: If $k=1$, this is highly false and this phenomena gives

rise to a new kind of Galois representations recently studied by Mazur and Wiles (cf.[22], last paragraph).

In fact, there is a more precise control theorem for each character:

For any $r>0$, let $\Gamma_r = \Gamma^{p^{r-1}}$. We can decompose $\omega_{k,r}(T)$ in product of linear factors in $\mathcal{O}_K[T]$ where $\mathcal{O}_K$ is the ring of integers of a finite extension $K/\mathbb{Q}_p$ containing $(p^{r-1})^{th}$ roots of unity :

For ε any character of Γ/Γ_r, set $P_{k,\varepsilon}(T) = 1+T-\varepsilon(u).u^k$, then

$$\omega_{k,r}(T) = \prod_{\varepsilon\in\Gamma/\Gamma_r} P_{k,\varepsilon}(T) \quad .$$

Set $\begin{cases} S^{ord}_{k,\varepsilon} = \text{largest } \mathcal{O}_K\text{-submodule of } S^{ord}_{k,r}(\mathcal{O}_K) \text{ on which } \Gamma \text{ acts via } \varepsilon. \\ h^{ord}_{k,\varepsilon} = \mathcal{O}_K\text{-subalgebra of End } S_{k,r}(\mathcal{O}_K) \text{ generated by the } T(n)\text{'s.} \end{cases}$

we see immediately that $S^{ord}_{k,\varepsilon} \subset (\bar{S}\otimes\mathcal{O}_K)[P_{k,\varepsilon}(T)]$; so that we have a natural $\mathcal{O}_K$-algebra morphism :

$$(1.8) \qquad (h^{ord}\otimes\mathcal{O}_K)/P_{k,\varepsilon}(T).(h^{ord}\otimes\mathcal{O}_K) \longrightarrow h^{ord}_{k,\varepsilon} \quad .$$

Theorem 1.8: If $r>0$, $k>1$, the map (1.8) is an isomorphism.

Remark : In fact, it is easy to check that theorem 1.7 and 1.8 are equivalent.

The next topic dealt with in Hida's theory is the concept of primitive component of the Hecke algebra. Let $\mathcal{L}$ be the field of fractions of Λ. The $\mathcal{L}$-algebra $h^{ord}\otimes\mathcal{L}$ is finite dimensional; hence it can be decomposed into a product of local $\mathcal{L}$-algebras. Let $\mathcal{X}$ be one of these components :

$$(1.9) \qquad h^{ord}\otimes\mathcal{L} \simeq \mathcal{X} \times \mathcal{A}$$

Set $h_1 = Im(pr_1 : h^{ord} \longrightarrow \mathcal{X})$, $h_2 = Im(pr_2 : h^{ord} \longrightarrow \mathcal{A})$.

By theorem 1.5, we see that the map (1.9) induces an injection

$$(1.10) \qquad h^{ord} \to h_1 \times h_2 \ .$$

Let $k>1$, $r>0$; extend the scalars to $K \supset \mu_{p^{r-1}}$,and set :

$$F_{k,\varepsilon} = ((h_1 \otimes \mathcal{O}_K) / P_{k,\varepsilon} \cdot (h_1 \otimes \mathcal{O}_K)) \otimes K \ .$$

Because of theorem 1.8, this K-algebra is a direct factor algebra of $h^{ord}_{k,\varepsilon} \otimes K$.

The control of primitivity is contained in the following theorem :

Theorem 1.9: 1). The following conditions are equivalent :

(i) There exists a couple (k_0,ε_0) , $k>1$, $\mathrm{Ker}\ \varepsilon_0 \supset \Gamma_r$, such that each character of K-algebras from F_{k,ε_0} to $\bar{\mathbb{Q}}_p$ (a fixed algebraic closure of $\mathbb{Q}_p$) induces an eigenform in $S^{ord}_{k,\varepsilon_0} \otimes \bar{\mathbb{Q}}_p$ whose level in Atkin-Lehner-Miyake sense is a multiple of N.

(ii) For each couple (k,ε), $k>1$, $r>0$, $\mathrm{Ker}\ \varepsilon \supset \Gamma_r$, all eigenforms attached to characters : $F_{k,\varepsilon} \to \bar{\mathbb{Q}}_p$ have level divisible by N.

2). When these conditions are fulfilled, $\mathcal{X}$ is a field and each algebra $F_{k,\varepsilon}$ is semi-simple.

We say then that the component $\mathcal{X}$ is primitive. Each eigenform in $S_{k,\varepsilon}(K)$ coming from some primitive $F_{k,\varepsilon}$ is called ordinary primitive.

Remark : One proves that if $r>1$, the ordinary-primitive eigenforms in $S_{k,r}$ are exactly the ordinary and primitive ones , however, when $r=1$, some ordinary-primitive forms are not primitive in the usual sense. To see an example, take any primitive form in the usual sense in $S_k(\Gamma_1(N))$, such that

$a(p,f)$ is a p-adic unit in $\bar{\mathbb{Q}}_p$ for some embedding of $\bar{\mathbb{Q}}$ into $\bar{\mathbb{Q}}_p$,write $a(p,f_0)= \alpha_p+\beta_p$, with $|\alpha_p|_p=1$ and $|\beta_p|_p<1$, and define $f(z)$ to be $f_0(z)- \beta_p.f_0(pz)$. Then it has level Np, is ordinary-primitive but not primitive.

Theorem 1.9 gives a criterion to prove that a component is primitive : it suffices to test it for one couple (k_0,ε_0).

Finally , we come to the definition of the Congruence Module attached to a primitive component of h^{ord}. Consider such a component $\mathcal{X}$ and set $C_0(\mathcal{X})$ to be the cokernel of the map (1.10).

We call this module the Congruence Module of $\mathcal{X}$. It results immediately from the definition that it is a finitely generated and torsion Λ-module.We may give another useful definition of it. Since Λ is a complete local noetherian ring , the finite Λ-algebra h^{ord} splits into the product of its localizations at maximal ideals. Let R be the local component of h^{ord} through which the first projection pr_1: $h^{ord} \to h_1$ factorises. We still get a decomposition :

$$(1.11) \qquad R\otimes \mathcal{L} \simeq \mathcal{X} \times \mathcal{B} \ ;$$

then, by setting R_i = Im $(pr_i|_R)$, we may still write:

$$C_0(\mathcal{X}) = \text{Coker } (R \to R_1 \times R_2)$$

This allows us to state a control theorem for the congruence module under some hypotheses:

Let (k,ε) as before and $h^{ord}_{k,\varepsilon} \otimes K = F_{k,\varepsilon} \times A_{k,\varepsilon}$ (this is allowed by theorem 1.9 since $\mathcal{X}$ is primitive); set $h_{k,1}$= Im $(h^{ord}_{k,\varepsilon} \to F_{k,\varepsilon})$ and $h_{k,2}$ = Im $(h^{ord}_{k,\varepsilon} \to A_{k,\varepsilon})$, then, we have:

$$(1.12) \qquad h^{ord}_{k,\varepsilon} \to h_{k,1} \times h_{k,2}$$

Define $C_{k,\varepsilon}$ as the cokernel of the map (1.12) (cf. Doi-Ohta [5]). This is a finite length $\mathcal{O}_K$-module .

Theorem 1.10 : Under the following hypothesis :

(i) h_1 is integrally closed,

(ii) R is a Gorenstein ring,

there exist natural isomorphisms :

$$C_0(\mathcal{X})/P_{k,\varepsilon}.C_0(\mathcal{X}) \to C_{k,\varepsilon} \ , \ C_0(\mathcal{X})/\omega_{k,r}.C_0(\mathcal{X}) \to C_{k,r}$$

Commentary : To check the hypotheses, we can test the first one by reducing h_1 modulo any fixed couple (k_0,ε_0): if the reduction is integrally closed, then so is h_1 itself. However, condition (ii) is much more difficult to check and its study uses algebro-geometric tools. We will explain, when it occurs, how to deal with this problem.

Nevertheless, in the situation we will study, we can prove Gorenstein-ness of R but h_1 might not be integrally closed. This is not crucial because we don't use the control of the Congruence Module in this work; however, since this is the main result in [10], we will briefly explain how it may be generalized even if h_1 is not integrally closed, provided R is Gorenstein. This is proved in a recent paper of Hida (cf.[39] theo. 4.1, 4.3, 4.4).

Let I be the integral closure of h_1 in $\mathcal{X}$. The new congruence module is defined by replacing the decomposition (1.11) by

$$(1.11^{bis}) \qquad R\otimes\mathcal{X} \simeq \mathcal{X}\times\mathcal{B}' .$$

More precisely, we write $\mathcal{X}\otimes_{\mathcal{L}_L}\mathcal{X} = \mathcal{X}\oplus\mathcal{X}'$, for some semi-simple $\mathcal{X}$-algebra $\mathcal{X}'$, the first projection being the obvious

multiplication map: $x\otimes y \to x.y$. We have $\mathcal{B}' = \mathcal{K}' \oplus \mathcal{B}\otimes\mathcal{K}$.

We have still an embedding of $R\otimes I$ into $I\oplus R_2'$ where $R_2' = \mathrm{Im}(pr_2: R\otimes I \to \mathcal{B}')$. Note that $R\otimes I$ and $I\otimes I$ are still local, and the first projection in (11^{bis}) factorises into the characters $R\otimes I \to I\otimes I$ and $m: I\otimes I \to I$, the latter being the multiplication map. Let c_1 be the ideal in R, kernel of $pr_2: R \to \mathcal{B}$. It is also an ideal in $R_1 = h_1$ and we see easily that $C_0(\mathcal{K}) = R_1/c_1$. We set

$$(1.13) \qquad C_0(\mathcal{K}, I) = \mathrm{Coker}(R\otimes I \to I\oplus R_2')$$

Set $\mathfrak{C}_1$ for the ideal in $R\otimes I$ which is the kernel of $pr_2: R\otimes I \to \mathcal{B}'$. It is likewise an ideal in $I = I\oplus\{0\} \subset I\oplus R_2'$ and similarly, we have $C_0(\mathcal{K}, I) = I/\mathfrak{C}_1$. Finally, set $C_0(m, I) = \mathrm{Coker}(I\otimes I \to I\oplus I')$; where $I' = \mathrm{Im}(I\otimes I \to \mathcal{K}')$.

In the context we will set in next paragraph, we have $R_1 = I$, and, following [40], in our particular case, we obtain in §8 below the relation between those I-modules:

$$0 \to C_0(m, I) \to C_0(\mathcal{K}, I) \to C_0(\mathcal{K}) \to 0$$

Now, to state the control theorem of $C_0(\mathcal{K}, I)$ when R is Gorenstein, we have to reduce modulo height one ideals in I instead of Λ (or Λ_L). We only consider primes P in I above $P_{k,\varepsilon}(T)$ in Λ_L, for $k>1$, $r>0$, such that $I/P \simeq \mathcal{O}_L$; that is of residual degree one over Λ_L. For instance, if $I = \mathcal{O}_L[[X]]$ with $(1+T)=(1+X)^{p^d}$, we have $P(X) = 1+X-\varepsilon'(\sqrt[p^d]{u}).\sqrt[p^d]{u}$, assuming of course that $\sqrt[p^d]{u}\in L$ and ε' running over the set of prolongations to $(1+p\mathbb{Z}_p)^{1/p^d}$ of the character ε of $(1+p\mathbb{Z}_p)$. Then, we have, in analogy with Theo.1.8: The natural morphism

$h^{ord}{}_{\otimes I}/P.(h^{ord}{}_{\otimes I}) \to h^{ord}_{k,\varepsilon}$ is an isomorphism for $k>1$, $r>0$. Then, by reducing mod.P the inclusion $R\otimes I \to I \oplus R'_2$, we obtain:

$$(R\otimes I)/P.(R\otimes I)\otimes L \simeq Lx\ B'_{k,\varepsilon}$$

This defines a congruence module C_P which we want to interpolate for varying P. Then, theorem 1.10^{bis} reads:

Theorem 1.10^{bis}: If R is Gorenstein, then there are canonical isomorphisms:

$$C_0(\mathcal{X},I)/P.C_0(\mathcal{X},I) \simeq C_P$$

where P is a prime of height one in I above $P_{k,\varepsilon}(T)$ for $k>1, r>0$.

Remark: Note that $\mathfrak{C}_1$ is a reflexive I-module; so, if I is a regular (which will be our case) hence factorial, $\mathfrak{C}_1$ will be a principal ideal.

In the next paragraph, we will see an application of Hida's theory, starting from a number-theoretic situation.

2. Component of h^{ord} of C.M. type attached to a Grössencharacter of an imaginary quadratic field.

All the number fields in the following are supposed to be given together with (compatible) embedding into $\mathbb{C}$; in particular , $\bar{\mathbb{Q}}$ denotes the field of algebraic numbers in $\mathbb{C}$. Let M be an imaginary quadratic field of discriminant -D, ring of integers $\mathcal{O}$; the order of the group of units $\mathcal{O}^\times$ is written 2e, e being equal to 1 except for $M=\mathbb{Q}(\sqrt{-1})$ (e=2) or $M=\mathbb{Q}(\sqrt{-3})$ (e=3). The class number is denoted by h (not necessarily equal to one as we suppposed in the introduction for simplicity). We give ourselves a Grössencharacter λ of M of type $(\nu,0)$ and conductor $\mathfrak{f}$. It means that λ is a homomorphism from the group of fractional ideals prime to $\mathfrak{f}$ with values in $\bar{\mathbb{Q}}$, such that for any ideal $\mathfrak{a}=(\alpha)$, with $\alpha\equiv 1 \bmod^\times \mathfrak{f}$, we have $\lambda(\mathfrak{a})=\alpha^\nu$, and the ideal $\mathfrak{f}$ is minimal so that this condition holds. We denote by L_0 the field generated by the values of λ.

Let p be a prime number >3, in all the rest of this work, we always assume that it splits in M : $p\mathcal{O} = \mathfrak{p}\mathfrak{p}^\rho$, ρ denoting complex conjugation in M. We fix an embedding ι_p of $\bar{\mathbb{Q}}$ in a fixed algebraic closure $\bar{\mathbb{Q}}_p$ of $\mathbb{Q}_p$ which induces a continuous map on M for the p-adic topology. We denote by L the closure in $\bar{\mathbb{Q}}_p$

of $\iota_p(L_0)$. We fix as prime to p-level the integer N=D.Norm(f). We are going to define a primitive component of h_L^{ord}= $h^{ord}(Np^\infty,\mathcal{O}_L)$ associated to (λ,ι_p) and deal with its congruence module. We make for this purpose the assumption that p doesn't divide ν.

For any integer r>0, let G_r be the ray class group of conductor $f.p^r$. Set $G_\infty = \varprojlim_r G_r$ the inverse limit of these groups for the obvious transition maps. Let $\mathcal{C}(G_\infty,\mathcal{O}_L)$ be the $\mathcal{O}_L$-module of continuous functions from G_∞ to $\mathcal{O}_L$ viewed as a Banach module for the norm $\|f\| = \sup_{g\in G_\infty} |f(g)|_p$. The algebra $\mathcal{O}_L[[G_\infty]]$ acts on it by (linearization of) translation maps: for [g] in G_∞(inside $\mathcal{O}_L[[G_\infty]]$) and f in $\mathcal{C}(G_\infty,\mathcal{O}_L)$, $f|[g](g') = f(gg')$. Furthermore, we have Mahler's theorem:

Theorem 2.1: We have a perfect continuous pairing:

$$(2.1) \qquad \langle\ ,\ \rangle : \mathcal{C}(G_\infty,\mathcal{O}_L)\times \mathcal{O}_L[[G_\infty]] \longrightarrow \mathcal{O}_L$$

such that $\langle f|[g],g'\rangle = \langle f,gg'\rangle$.

Proof: We may decompose G_∞ as the direct product of a finite group G_t and a group W which is isomorphic to $\mathbb{Z}_p$. Then, we have:

$$\mathcal{O}_L[[G_\infty]] \simeq \mathcal{O}_L[[T]][G_t], \qquad \mathcal{C}(G_\infty,\mathcal{O}_L) \simeq \mathcal{C}(\mathbb{Z}_p,\mathcal{O}_L)\otimes \mathcal{F}(G_t,\mathcal{O}_L),$$

the tensor product being taken over $\mathcal{O}_L$ and $\mathcal{F}(G_\infty,\mathcal{O}_L)$ being the module of all the functions from G_t to $\mathcal{O}_L$. The classical Mahler's theorem asserts that the Hilbert polynomials $\binom{x}{n} = \frac{x(x-1)\ldots(x-n+1)}{n!}$ for n=0,1,... form a normal basis of the Banach module $\mathcal{C}(\mathbb{Z}_p,\mathcal{O}_L)$ with the usual supremum norm $\|f\|$=

$\sup_{x\in\mathbb{Z}_p} |f(x)|$ (cf. [17]). So, we have a perfect duality:

$$\mathscr{C}(\mathbb{Z}_p,\mathcal{O}_L)\times \mathcal{O}_L[[T]] \to \mathcal{O}_L$$

given by $(f,\sigma) \to \sum_{n\geq 0} a_n c_n$, for $f = \sum_{n\geq 0} a_n \binom{x}{n}$, $\sigma = \sum_{n\geq 0} c_n T^n$.

The property $\langle f|(1+T),\sigma\rangle = \langle f,(1+T).\sigma\rangle$ is easy to see if we notice that $f|(1+T)(x)=f(x+1)$ and $\binom{x+1}{n} = \binom{x}{n} + \binom{x}{n-1}$.

We then define the total pairing by $\langle \sum_{g_t\in G_t} f_{g_t}[g_t], \sum_{g_t\in G_t} \sigma_{g_t}\otimes\delta_{g_t}\rangle$

$\sum_{g_t\in G_t} \langle f_{g_t}, \sigma_{g_t^{-1}}\rangle$ where we denote by δ_{g_t} the delta function at g_t in G_t. The required bilinearity and the perfectness follow then immediately from this definition.

We call $\mathscr{C}(G_\infty,\mathcal{O}_L)$ the module of p-adic cusp forms for $GL_{1/M}$ with coefficients in $\mathcal{O}_L$; similarly, we call $\mathcal{O}_L[[G_\infty]]$ the p-adic Hecke algebra for $GL_{1/M}$. In the $GL_{2/\mathbb{Q}}$-case, we also have a perfect continuous pairing generalizing (1.1) :

(2.2) $\langle\ ,\rangle: \bar{S}(\mathcal{O}_L)\times h_L \to \mathcal{O}_L$, $(f,T) \to a(1,f|T)$,

satisfying also the bilinearity $\langle f|T,T'\rangle = \langle f,TT'\rangle$ (cf. [10] §3).

We then consider the p-adic base change map:

$$GL_{1/M} \to GL_{2/\mathbb{Q}}$$

$$\theta : \mathscr{C}(G_\infty,\mathcal{O}_L) \to \bar{S}(Np^\infty,\mathcal{O}_L) \ , \ f \to \theta(f) = \sum_{a\in I} f(a)q^{Na}$$

where I is the monoid of ideals in $\mathcal{O}$ (integers in M) prime to fp. It is easy to verify that I embeds into G_∞ by the obvious map. Now, θ is a continuous map of Banach $\mathcal{O}_L$-modules. We dualize it and because of the bilinearity conditions in (2.1) and (2.2), we obtain a morphism of $\mathcal{O}_L$-algebras:

$$\theta^*: h(Np^\infty,\mathcal{O}_L) \to \mathcal{O}_L[[G_\infty]]$$

given, on Hecke operators $T(\ell)$ with ℓ rational prime, by:

$$T(\ell) \longrightarrow \begin{cases} [\mathfrak{L}]+[\mathfrak{L}^{\rho}] & \text{if } \ell \text{ is decomposed in M and } (\ell, f\ p)=1 \\ 0 & \text{if } \ell \text{ is inert in M} \\ [\mathfrak{L}] & \text{if } \ell \text{ is ramified or splits but } \mathfrak{L}^{\rho} \mid fp. \end{cases}$$

Now, we use the datum of λ as homomorphism from I to $\bar{\mathbb{Q}}_p^x$.

$$\lambda : I \longrightarrow L_0^x \subset L^x \subset \bar{\mathbb{Q}}_p^x.$$

We can extend it by p-adic continuity to G_∞ so that we get:

$$\hat{\lambda} : G_\infty \longrightarrow \mathcal{O}_L^x.$$

This is an alternative definition of the p-adic avatar of a Grössencharacter of type (A_0) constructed by Weil in [37].

With this tool, we define a morphism η of $\mathcal{O}_L$-algebras :

$$:\mathcal{O}_L[[G_\infty]] \longrightarrow \mathcal{O}_L[[W]]$$

We have non-canonically $G_\infty \simeq G_t \times W$ but inside W there is a canonical subgroup Γ of G_∞ : namely the inverse limit of the p-Sylow in $(\mathcal{O}/_{p^r})^x \subset (\mathcal{O}/_{fp^r})^x$ viewed as subgroup of G_r , r=1,2...Let $p^d=(W:\Gamma)$. Choose a topological generator w of W such that $w^{p^d} = u = 1+Np \in \Gamma$, the topological generator of Γ we fix once for all. This furnishes compatible isomorphisms $\mathcal{O}_L[[W]] \simeq \mathcal{O}_L[[X]]$, $\mathcal{O}_L[[\Gamma]] \simeq \mathcal{O}_L[[T]]$, and the inclusion induced by $\Gamma \subset W$ corresponding to $(1+T) \longrightarrow (1+X)^{p^d}$.

Now, for $g \in G_\infty = G_t \times W$, $g = (g_t, w')$, let $\hat{\lambda}_t(g) = \hat{\lambda}(g_t)$, $\hat{\lambda}_0(g) = \hat{\lambda}(w')^{1/\nu}$. The character $\hat{\lambda}_0$ sends u to $u = \hat{\lambda}_0(w)^{p^d}$. We set:

$$\eta(g) = \hat{\lambda}_t(g).\hat{\lambda}_0(g)^{-1}.[w'].$$

By this definition, it is obvious that η is surjective.

Note also that $\mathcal{O}_p^x = \varprojlim (\mathcal{O}/p^r)^x$ naturally injects into G_∞.

We finally note $\Lambda_L = \mathcal{O}_L[[T]] = \Lambda \otimes \mathcal{O}_L$. It is obvious from (1.7) that $h(Np^\infty, \mathcal{O}_L)$ is a Λ_L-algebra (so is its ordinary part of

course). For any integer $k'>1$, any $r\geq 0$, and any character ε of Γ of conductor p^r, we set $P_{k',\varepsilon}(X) = 1+T - \varepsilon(u)u^{k'}$, $[u = 1+Np]$.

Theorem 2.2: The map $\chi = \eta o\theta^*$: $h(Np^\infty,\mathcal{O}_L) \to \mathcal{O}_L[[W]]= \mathcal{O}_L[[X]]$ factorizes through the ordinary part of h^{ord} into a morphism of Λ_L-algebras, which is surjective if $0<\nu<p-1$. For any $k'>1$ and ε any character of Γ of conductor, say, p^r, the reduction mod.$P_{k',\varepsilon}(T)$ of χ gives rise to characters : $h_{k'}(\Gamma_1(Np^r),\mathcal{O}_L) \to \bar{\mathbb{Q}}_p$ associated with the series $\theta(\hat{\lambda}_t.\lambda_0^{k'-1}.\varepsilon')$, where ε' runs over the set of characters in W whose restriction to Γ equals ε.

Proof : We have $\theta^*(T(p)) = [p^\rho]$ by (2.2); so χ factorizes through the ordinary part of $h(Np^\infty,\mathcal{O}_L)$. We are going to check the Λ_L-linearity of χ and the formula for the reduction mod.$P_{k',\varepsilon}(T)$ simultaneously. After some extension of scalars from L to a field K containing $\mu_{p^{r+d}}$, we can apply theorem 1.9 in order to reduce χ mod.$P_{k,\varepsilon}(T)$. We obtain a character $\chi_{k',\varepsilon}$: $h_{k,\varepsilon}(K) \to K[X]/(1+T - \varepsilon(u)u^{k'})$; so we get characters $\chi_{k',\varepsilon'}$: $h_{k',\varepsilon'}(K) \to K$ by reducing mod.$(1+X-\varepsilon'(w)\hat{\lambda}_0(w))$. It is clear that the series corresponding to such a character is $\theta(\hat{\lambda}_t.\hat{\lambda}_0^{k'-1}.\varepsilon')$. So the diamond of weight k' of a rational prime ℓ is sent by $\chi_{k',\varepsilon'}$ on $\left(\frac{-D}{\ell}\right).\dfrac{\hat{\lambda}_t.\hat{\lambda}_0^{k'-1}.\varepsilon'((\ell))}{\ell^{k'-1}}$.

Consequently, the diamond of weight 0 of an element $\ell\equiv 1$ mod.Np is sent to the element of $\mathcal{O}_L[[X]]$ congruent to $(1+T)^{\log_p \ell}$ mod.$(1+X - \hat{\lambda}_0(w)\varepsilon'(w))$ for all k' and ε': $\chi(\langle\ell\rangle_0)= (1+X)^{\log_p \ell}= \langle\ell\rangle_0$.

This implies the Λ_L-linearity. It now remains to check

the surjectivity. We first prove surjectivity of $\chi\otimes Id_{\mathcal{L}_L}$ where $\mathcal{L}_L$ denotes the field of fractions of Λ_L.

By duality, it is enough to prove that $Ker(\theta\otimes Id_L)$ is finite dimensional as L-vector space.

In fact, if this is true, the theory of duality between Banach spaces implies that $Coker(\theta\otimes Id_L)^*$ is the dual of $Ker(\theta\otimes Id_L)$, so is finite dimensional and if we tensor by the field of fractions of Λ_L, we get the surjectivity of $\theta\otimes Id_{\mathcal{L}_L}$. So, take a continuous map $f: G_\infty \dashrightarrow L$ such that $\theta(f)=0$.

Fact : If $\theta(f)=0$, f is constant in each coset of G_∞ mod.$\mathcal{O}_p^x$

Proof : Consider the exact sequence $0 \to \mathcal{O}_p^x \dashrightarrow G_\infty \to G_f \to 0$, where G_f denotes the ray class group of M modulo f. Fix a complete system of representatives of G_f, say S, in I, all elements of which being prime to pff^ρ.

Set $P=\{\mathfrak{a}\in I;\ \mathfrak{a}=(\alpha)\ \alpha\equiv 1 \bmod f,\ (\alpha,pf^\rho)=1\}$.

We will use Cebotarev's density theorem to deduce from the equality $f(\mathcal{L})+f(\mathcal{L}^\rho)=0$ for all rational prime ℓ decomposed in M and prime to fp, that $f(\mathfrak{a}(\alpha))$ is constant for a fixed $\mathfrak{a}\in S$ and (α) running in $P\cap \mathfrak{a}^{-1}I$. Let M_{fp^r} (resp. $M_{f^\rho p^{\rho r}}$) be the ray class field of M of conductor fp^r (resp. $f^\rho p^{\rho r}$). Let σ be the automorphism of the compositum of those two fields whose restriction to M_{fp^r} is $(\mathfrak{a}(\alpha),M_{fp^r}/M)$ and to $M_{f^\rho p^{\rho r}}$ is $(\mathfrak{a},M_{f^\rho p^{\rho r}}/M)$; it exists because the intersection of those fields is $M_{(f^\rho,f)}$ and $\alpha\equiv 1 \bmod.(f^\rho,f)$. So, by Cebotarev's density theorem, there exists a prime ideal $\mathcal{L}$ of degree one in

M such that $(\mathcal{L},M_{\mathfrak{f}p^r}/M)=\sigma|_{M_{\mathfrak{f}p^r}}$ and $(\mathcal{L},M_{\mathfrak{f}^{\rho}p^{\rho r}}/M)=\sigma|_{M_{\mathfrak{f}^{\rho}p^{\rho r}}}$ so that $\mathcal{L}\equiv a(\alpha) \bmod P_{\mathfrak{f}p^r}$, $\mathcal{L}^{\rho}\equiv a^{\rho} \bmod P_{\mathfrak{f}p^r}$; thus, by letting r grow to the infinity, we obtain $f(a(\alpha)) = -f(a^{\rho})$.

This proves the generic surjectivity. We now deduce from this the surjectivity. Note that since $\chi(\langle\zeta\rangle_0)=\zeta^{\nu+1}$ by the above computations, χ factorizes through $h^{ord}(a)$ where $a\equiv\nu+1$ mod.p-1, and $\theta^*(h^{ord}(\nu+1)) \subset \mathcal{O}_L[[G_\infty]](\nu)= \{x\in\mathcal{O}_L[[G_\infty]];[\zeta].x = \zeta^{\nu}x$, for all $\zeta\in\mu_{p-1} \subset \mathcal{O}_p^x \subset G_\infty\}$. So we only have to check the injectivity of θ restricted to the ν-part of $\mathcal{C}(G_\infty,\mathcal{O}_L)$, i.e. the set of $f: G_\infty \to \mathcal{O}_L$ such that for all ζ in $\mu_{p-1} \subset G_\infty$, $f(\zeta g)=\zeta^{\nu}f(g)$. By the proof above, if $\theta(f)=0$, then $\mathcal{O}_p^x$ acts trivially on f; hence $\mu_{p-1} \subset \mathcal{O}_p^x$ acts also trivially. Since $\nu\not\equiv 0$ mod.p-1, we see that f=0. We conclude that θ^* and χ are surjective.

Corollary 2.4 : The surjective character $\chi : h_L^{ord} \to \mathcal{O}_L[[X]]$ defines a primitive component of h_L^{ord} of degree p^d.

Proof : By the criterion of primitivity of th.1.9, we have only to check primitivity modulo some P_{k_0,ε_0}. Take k_0 to be $\nu+1$ and ε_0 to be trivial. Then the algebra F_{k_0,ε_0} is $L[X]/(1+T-u^{\nu+1})$ which is semi-simple and whose characters correspond to the series $\theta(\hat{\lambda}\varepsilon')$ (the ε''s are the characters of p-power order of G_1). By a well-known theorem of Hecke, these are ordinary-primitive cusp forms of weight $\nu+1$. The degree of the component $\mathcal{O}_L[[X]]\otimes\mathcal{L}$ is p^d.

We denote this component by $\mathcal{X}$, and R will stand for the local

component in h^{ord} through which χ factorises. Hence, we are in the situation of theorem 1.9 (after replacing the ground ring $\mathbb{Z}_p$ by $\mathcal{O}_L$). This component $\mathcal{X}$ is called component of C.M. type attached to (λ, ι_p). We consider also the Λ_L- module of congruence $C_0(\mathcal{X})$ attached to it. It can still be written R_1/c_1 where $R_1 = h_1 = \mathcal{O}_L[[X]]$ by cor.2.4. Note that c_1 is a reflexive Λ_L-module (being the trace of h^{ord} on $\mathcal{X}$), so it is also free over $\mathcal{O}_L[[X]]$ i.e. principal: $c_1 = (H_{(\lambda, \iota_p)}(X))$.

In order to get further informations on R, we will assume some hypotheses about the Grössencharacter λ and the prime p (splitting in M at least, since the beginning of the paragraph).

Hypotheses 2.5 :The conductor $\mathfrak{f}$ of λ is prime to its conjugate $\mathfrak{f}^{\rho}$, p doesn't divide $6N\varphi(N)$ and $\nu+1<p-1$.

Thanks to those hypotheses, we prove in the next paragraph the

Theorem 2.6 : 1.The component R is a Gorenstein ring.

2.The new Congruence Module $C_0(\mathcal{X}, I)$ is controlled in the sense of theorem 1.10^{bis}.

So , the next topic is the study of some Gorenstein-ness criterions to prove theorem 2.6. under hypotheses 2.5.

3. Gorenstein-ness of the local component associated to χ.

First, recall general facts about Gorenstein rings.

Definition 3.1 : Let R be any local noetherian ring with maximal ideal $\mathfrak{M}$ and residual field k, of Krull dimension d. We say that R is Gorenstein if it is Cohen-Macaulay and $\mathfrak{M}$ contains an irreducible ideal generated by a regular sequence of length d. Recall that an ideal is said irreducible if it cannot be written as intersection of two strictly bigger ideals.

Lemma 3.2 : R is Gorenstein iff : $\mathrm{Ext}^i(k,R) = \begin{cases} 0 \text{ if } i<d \\ k \text{ if } i=d \end{cases}$.

Proof : Let $(x_1,\ldots,x_d)$ be a regular sequence in $\mathfrak{M}$ generating an irreducible ideal I. First, from the very existence of the regular sequence, we deduce that $\mathrm{Ext}^i(k,R)=0$ for all $i<d$ (cf. (15.B) theorem 26 of [19]). Now, R/I is local artinian (dim.0) We have $\mathrm{Hom}(k,R/I)=k$ because of the irreducibility hypothesis. But, by induction using the exact sequence $0 \to R^{(i-1)} \to R^{(i-1)} \to R^{(i)} \to 0$ (multiplication by x_i) for $R^{(i)} = R/(x_1,\ldots,x_i)$, we get $\mathrm{Ext}^d(k,R) = \mathrm{Ext}^{d-1}(k,R^{(1)}) = \ldots = \mathrm{Ext}^0(k,R^{(d)}) = k$. The converse is proved by reading the previous proof in the reverse direction.

Proposition 3.3 : Let R be local noetherian and $\rho \in R$ which doesn't divide zero. Then

(i) R is Gorenstein of dimension d if and only if $R/\rho R$ is Gorenstein of dimension d-1.

(ii) If R is artinian with finite residual field, R is

Gorenstein (of dimension 0) if and only if its Pontryagin dual is R-free of rank 1.

(iii) If R is a finite free $\mathbb{Z}_p$-algebra, R is Gorenstein if and only if $\mathrm{Hom}(R,\mathbb{Z}_p)$ is R-free of rank 1.

Proof : (i) is clear by taking the long Ext-exact sequence attached to $0 \to R \xrightarrow{(x\rho)} R \to R/\rho R \to 0$.

(ii) : Let R^* be the Pontryagin dual of R ; R is Gorenstein of dimension 0 iff $\mathrm{Hom}(k,R)$ is of dimension 1 i.e. if the $\mathfrak{M}$-torsion in R, $R[\mathfrak{M}]$ is $\simeq k$; on the other hand, since k is finite, the trace map induces a k-linear isomorphism between k and its Pontryagin dual; so, $R[\mathfrak{M}] \simeq k$ is equivalent to $R^*/\mathfrak{M}.R^* \simeq k$, and finally to $R^* \simeq R$ as R-module by Nakayama's lemma.

(iii): By flatness of R over $\mathbb{Z}_p$, p doesn't divide zero in R; so, the $\mathbb{Z}_p$-algebra R is Gorenstein of dimension 1 iff R/pR is Gorenstein of dimension 0; hence by (ii), iff $\mathrm{Hom}(R/pR,\mathbb{F}_p) \simeq R/pR$. But, by Nakayama's lemma, this is equivalent to $\mathrm{Hom}(R,\mathbb{Z}_p) \simeq R$.

After these preliminaries, let us consider a local component R of h_L^{ord} with maximal ideal $\mathfrak{M}$. It is finite and flat over Λ_L so it has Krull dimension 2. So, if we introduce the twisted Iwasawa polynomials $\omega_{2,r}(T) = (1+T)^{p^{r-1}} - u^{2p^{r-1}}$, the sequence $(\omega_{2,r}(T),p)$ is regular and by setting $R(r) = R/\omega_{2,r}.R$, we deduce easily from proposition 3.3 the following

Proposition 3.4 :The following assertions are equivalent:

(i) R(1) is Gorenstein of dimension 1.

(ii) For any $r \geq 1$, R(r) is Gorenstein of dimension 1.

(iii) R is Gorenstein of dimension 2.

(iv) $\mathrm{Hom}(R,\Lambda_L)$ is R-free of rank one.

Proof : (i),(ii),(iii) are obviously equivalent from prop.3.5 ,(i). Then, equivalence with (iv) comes from $\mathrm{Hom}_{\mathcal{O}_L}(R(1),\mathcal{O}_L)\simeq \mathrm{Hom}_{\mathbb{Z}_p}(R(1),\mathbb{Z}_p)$ as R(1)-module (via: $(f:R_1\to\mathcal{O}_L)\to \mathrm{Tr}_{L/\mathbb{Q}_p}(\delta_{L/\mathbb{Q}_p}^{-1}.f)$, where $\delta_{L/\mathbb{Q}_p}$ is the different of $L/\mathbb{Q}_p$).

Let $\mathfrak{M}$ be the maximal ideal of the arbitrary local component R and k its residual field. The field k is also the residual field of $\mathcal{O}_L$. We will recall a criterion for Gorenstein-ness of R proved by Mazur-Wiles(cf.[22] Prop.6.1) when N=1 and in [34] §4 in the general case, with some hypothesis however.

Definition 3.5 : Let $\bar{\rho}$: $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})\to \mathrm{GL}(V)$ be a Galois representation on a finite dimensional k-vector space. We say that $\bar{\rho}$ is $\mathfrak{M}$-residual attached to R if

(i) V is 2-dimensional over k.

(ii) $\bar{\rho}$ is unramified outside Np.

(iii) The characteristic polynomial of Frob_ℓ for $\ell\nmid Np$ is : $X^2-T(\ell)X-\ell\langle\ell\rangle_2 \bmod.\mathfrak{M}$.

Besides, if we let the group μ_{p-1} of $p-1^{st}$ root of unity in $\mathbb{Z}_p^{\times}$ inside Z (cf.§1 of[10]) act on $h^{ord}(Np^{\infty},\mathcal{O}_L)$ via diamond of weight 0, we can decompose :

$$h_L^{ord}=\oplus\, h_L^{ord}(a),\ a \text{ running in } \mathbb{Z}/(p-1)\mathbb{Z}\ ,\ \text{the}$$

Pontryagin dual of μ_{p-1}.

It is clear that the local component R is contained in some $h_L^{ord}(a)$ for a unique a in $\mathbb{Z}/(p-1)\mathbb{Z}$. Then our generalisation of

Mazur-Wiles criterion is:

Proposition 3.6 : Suppose $a \neq 1,2$.

If there exists an $\mathfrak{M}$-residual representation attached to R which is irreducible, then R is Gorenstein.

The proof involves another criterion of Gorenstein-ness of R_1 due to Mazur([] Prop.15.1):

Let $J_1(Np)_{/\mathbb{Q}}$ be the jacobian (Picard variety) of the modular curve $X_1(Np)_{/\mathbb{Q}}$ (the $\mathbb{Q}$-model is chosen such that the infinity cusp is $\mathbb{Q}$-rational). The Hecke algebra $h_2(\Gamma_1(Np),\mathbb{Z})$ acts on it by pull-back of divisor classes by the Hecke correspondences (for their definition, see [21] chap.2 §4 and [34]). The Galois group $Gal(\bar{\mathbb{Q}}/\mathbb{Q})$ acts on $J_1(Np)(\bar{\mathbb{Q}})$ by "Picard action" (see [35] §4 or §5 below).

We can form the R(1)-module $J_1(R)$ by considering $J_1(Np^\infty)[p]\otimes\mathcal{O}_L$ which is an $h_2(\Gamma_1(Np),\mathcal{O}_L)$-module and then taking its R(1)-part. Let finally $\mathfrak{M}_1$ be the maximal ideal of R(1). Then we have:

Proposition 3.7: If $J_1(R)[\mathfrak{M}_1]$ is 2-dimensional as k-vector space, then R(1)is Gorenstein (hence, so is R by proposition 3. 6).

Commentary:This criterion is valid without hypothesis about the component R.

Proof :Suppose $J_1(R)[\mathfrak{M}_1] \simeq k^2$. Let $Ta(J_1(R)) = \varprojlim J_1(R)[p^m]$. We first show that $Ta(J_1(R))$ is free of rank 2 over R(1). We know that there exists perfect bilinear pairings (compatible when m varies):

$$\langle\ ,\ \rangle : J_1(R)[p^m]\times J_1(R)[p^m] \to \mu_{p^m}\otimes\mathcal{O}_L$$

such that $\langle x|t,y\rangle = \langle x,y|t\rangle$ for any t in $h_2(\Gamma_1(Np),\mathcal{O}_L)$. However, be careful that they are not induced by the Weil pairing on $J_1(Np)$ but by its twist by the Weil involution of level Np : $\langle x,y\rangle_m = e_m(x,y|W_{Np})$.

On the other hand, is clear that $J_1(R)$ is a p-divisible group , so that we have exact sequences:

(*) $\quad 0 \to p^m.Ta(J_1(R)) \to Ta(J_1(R)) \to J_1(R)[p^m] \to 0$

In particular: $Ta(J_1(R))/\mathfrak{M}_1.Ta(J_1(R)) \simeq J_1(R)[p]/\mathfrak{M}_1.J_1(R)[p]$

So, by applying duality theory to the pairing $\langle\ ,\ \rangle_m$ for m=1, we obtain: $Ta(J_1(R))/\mathfrak{M}_1.Ta(J_1(R)) \simeq Hom_{\mathcal{O}_L}(J_1(R)[\mathfrak{M}_1],\mathcal{O}_L\otimes \mu_p)$ which is 2-dimensional over ℓ. Then by Nakayama's lemma, we have a surjective R(1)-linear map : $R(1)^2 \to Ta(J_1(R))$

Let us prove that it is injective. To check this, it is enough to tensor it by L because R(1) is $\mathcal{O}_L$-free. But it is well-known that $H^1(X_1(Np),\mathbb{Q}) \simeq h_2(\Gamma_1(Np),\mathbb{Q})^2$ as $h_2(\Gamma_1(Np),\mathbb{Q})$-module. So we get: $L\otimes Ta(J_1(R)) \simeq e_R.e.H^1(X_1(Np),L) \simeq (R(1)\otimes L)^2$

where e is the ordinary idempotent and e_R is the unit element of the local component R(1) of $h_2^{ord}(\Gamma_1 Np),\mathcal{O}_L)$. So, our two modules have the same rank over $\mathcal{O}_L$ hence the surjective map above is an isomorphism. Finally, by using the pairings $\langle\ ,\ \rangle_m$, and (*), we see :

$$Ta(J_1(R))/p^m.Ta(J_1(R)) \simeq Hom_{\mathcal{O}_L}(Ta(J_1(R)),\mathbb{Z}/p^m\mathbb{Z}\otimes\mathcal{O}_L)$$

as R(1)-modules, hence at the inverse limit, we obtain :

$$Ta(J_1(R)) \simeq Hom_{\mathcal{O}_L}(Ta(J_1(R)),\mathcal{O}_L).$$

This provides us an R(1)-linear isomorphism: $R(1)\oplus R(1) \simeq$

$R(1)' \oplus R(1)'$ where $R(1)' = \mathrm{Hom}_{\mathcal{O}_L}(R(1), \mathcal{O}_L)$. Let then $\pi_{i,j}$ be the four $R(1)$ -linear projections $R(1)' \to R(1)$. One at least among those four maps is surjective, otherwise $R(1)' \oplus R(1)' \subset \mathfrak{M}_1.(R(1) \oplus R(1)) = Ta(J_1(R))$ which is absurd. Take such a map; it is an isomorphism because of equality of $\mathcal{O}_L$-ranks. Q.E.D.

Now, to the proof of proposition 3.6. Suppose we have an $\mathfrak{M}$-residual irreducible representation of $Gal(\bar{\mathbb{Q}}/\mathbb{Q})$ on V.

We will prove that W is 2-dimensional.

Lemma 3.8 :Let G be a group, V a 2-dimensional G-irreducible module, W a ℓG artinian module, such that for any σ in G , the characteristic polynomial of σ_V annihilates σ_W (σ_V , resp. σ_W is the automorphism of V resp.W given by σ). Then, all quotients of a Jordan-Hölder sequence of W are isomorphic to V. That is $W^{s.s.} \simeq V^{(n)}$(direct sum of n copies of V).

Proof : Use the following standard trick: introduce W' the contragredient representation of W and $W'(\det \rho_V)$ its twist by the determinant of ρ_V: $G \to GL(V)$. Then the characteristic polynomial $P_{\sigma_M}(X)$ of σ acting on $M=W \oplus W'(\det\rho_V)$ is $P_{\sigma_V}(X)^{\dim W}$ because if $P_{\sigma_V}(X) = (X-\alpha)(X-\beta)$, we have: $P_{\sigma_W}(X) = (X-\alpha)^a(X-\beta)^b$, $P_{\sigma_{W'}}(X) = (X-\alpha^{-1})^a(X-\beta^{-1})^b$, $P_{\sigma_{W'(\det \rho_V)}}(X) = (X-\beta)^a(X-\alpha)^b$.

Then, the characteristic polynomials of M and $V^{(\dim W)}$ coincide; this implies, by Brauer-Nesbitt's theorem ([4]) that the semi-simplification of M is isomorphic to $V^{(\dim W)}$, so $W^{s.s.}$ is also isomorphic to some power of V.

We apply this lemma to our situation: V is $\ell Gal(\bar{\mathbb{Q}}/\mathbb{Q})$-

irreducible, $\dim_{\ell} V = 2$. The Eichler-Shimura relations show that for ℓ a rational prime, $\ell \nmid Np$, Frob_ℓ acting by Picard action on W is killed by $X^2 - T(\ell)X + \ell\langle\ell\rangle_2$ mod.$\mathfrak{M}$, which is the characteristic polynomial of Frob_ℓ on V. So, hypotheses of Lemma 3.8 are fulfilled, and we get $W^{s.s.} \simeq V^{(n)}$. Let us prove that n = 1. We use a structure theorem for $J_1(R)$ which is probably always true, but is only proved by using hypothesis $a \neq 1,2$. The version used here is a special case of Theorem 4.4 of [34]. We will come back to the more general version in §5 and explain shortly its proof.

Theorem 3.9: If $a \neq 1,2$, there exists an R(1)-isomorphism :

$$J_1(R) \simeq R(1) \otimes \mathbb{T}_p \oplus \mathrm{Hom}(R(1), \mathbb{T}_p)$$

where $\mathbb{T}_p$ denotes the p-adic torus $\mathbb{Q}_p/\mathbb{Z}_p$.

By using this result, we can write :

$$J_1(R)[p] \simeq R(1)/pR(1) \oplus \mathrm{Hom}(R(1)/pR(1), \mathbb{F}_p)$$

We remark that R(1)/pR(1) and $\mathrm{Hom}(R(1)/pR(1), \mathbb{F}_p)$ are artinian indecomposable R(1)-modules (they cannot be written as direct sum of non-trivial R(1)-modules)[This is obvious because the R(1)-endomorphism ring of both those modules is R(1)/pR(1) which is a local ring; hence, it cannot contain non-trivial idempotents i.e. projectors].

But, since $J_1(Np)$ is defined over $\mathbb{Q}$ and so are all Hecke correspondences, the complex conjugation c acts on $J_1(R)[p]$. We can henceforth decompose : $J_1(R)[p] = J_1(R)[p]^+ \oplus J_1(R)[p]^-$ where $J_1(R)[p]^{\pm} = \{x \in J_1(R)[p];\ cx = \pm x\}$.

Now, by Krull-Schmidt-Azumaya's theorem ([4]), we have :

$$\begin{cases} J_1(R)[p]^+ \simeq R(1)/pR(1) \\ J_1(R)[p]^- \simeq (R(1)/pR(1))' \end{cases} \quad \text{or} \quad \begin{cases} J_1(R)[p]^- \simeq R(1)/pR(1) \\ J_1(R)[p]^+ \simeq (R(1)/pR(1))' \end{cases}$$

where $V' = \mathrm{Hom}(V,\mathbb{F}_p)$.

We then take the $\mathfrak{M}_1$-torsion : $W^+ = J_1(R)[\mathfrak{M}_1] \simeq R(1)/pR(1)[\mathfrak{M}_1]$ and $W^- \simeq \mathrm{Hom}(k,\mathbb{F}_p) \simeq k$ (by the trace map).

Observe incidentally that according to Proposition 3.4, (ii), R(1)is Gorenstein iff the $\mathfrak{M}_1$-torsion of R(1)/pR(1) is 1-dimensional; but, without any supposition, we get $\mathrm{Hom}(R(1)/pR(1),\mathbb{F}_p)[\mathfrak{M}_1] \simeq k$.

Finally, we know that the complex conjugation can be approximated by Frobeniuses Frob_ℓ, $\ell \equiv -1$ mod.Np and from the definition of $\mathfrak{M}$-residuality, we obtain $\det \bar{\rho}(c) = -1$. So, since $p \neq 2$, $\bar{\rho}(c)$ is not a scalar on V and V^+ and V^- are 1-dimensional, so the number of + and - in W is n and is one for at least one of those signs : n = 1.Q.E.D.

In the end of this paragraph, we are going to apply this criterion to prove theorem 2.6.

Take the component R attached to the character χ in (2.5). First, we recall that the integer a modulo p-1 corresponding to R is $\nu+1$ which is neither 1 or 2 because of hypothesis 2.5. By reducing mod.$P_2(T)=1+T-u^2$, we obtain characters :

(3.5) $h_2(\Gamma_1 Np),\mathcal{O}_L) \to \bar{\mathbb{Q}}_p$, corresponding to the forms $\theta(\hat{\lambda}_t.\hat{\lambda}_0.\varepsilon'),\varepsilon'$ being any character of W/Γ .

The p-adic character $\hat{\lambda}_t.\hat{\lambda}_0 : G_\infty \to \mathcal{O}_L^\times$ is the p-adic avatar of the Grössencharacter of type (1,0) defined as follows :Since p>5, there is a Grössencharacter μ_0 of M of type (1,0) of conductor p. It yields a p-adic character $\hat{\mu}_0$ on G_∞. We can

twist it by a Dirichlet character ξ of G_1 to get $\hat{\lambda}_t.\hat{\lambda}_0$. Then the Grössencharacter $\mu = \xi.\mu_0$ fulfill the requirement. Then , if we set $f_{\varepsilon'} = \sum_{(a,fp)=1} \mu\varepsilon'(a).q^{Na}$, we have : $\theta(\hat{\lambda}_t.\hat{\lambda}_0.\varepsilon') = f_{\varepsilon'}(z)$.

Let $M(\mu\varepsilon')$ be the field generated by the values of $\mu\varepsilon'$.

Proposition 3.10 :The field $M(\mu\varepsilon')$ coincides with the field generated by the coefficients of $f_{\varepsilon'}$. The exact conductor of $\mu\varepsilon'$ is fp for any ε'; hence, $f_{\varepsilon'}$ is primitive of conductor Np.

Proof : Let $K(f_{\varepsilon'})$ be the field generated by the coefficients of $f_{\varepsilon'}$. We have obviously $K(f_{\varepsilon'}) \subset M(\mu\varepsilon')$. Furthermore $M \subset K(f_{\varepsilon'})$ because $a(p,f_{\varepsilon'}) = \mu\varepsilon'(p^{\rho})$, which generates M. In fact, $\mu\varepsilon'(p) = 0$, i.e. $\mu\varepsilon'$ is ramified at p. The reason for that is that $\iota_p o \mu\varepsilon'$ is congruent to $\hat{\lambda}_t.\hat{\lambda}_0$ modulo the maximal ideal of $\bar{\mathbb{Q}}_p$, so it coincides with $\zeta \dashrightarrow \zeta^{\nu+1}$ on $(\mathcal{O}/p)^x \subset G_\infty$; the inequality $1<\nu+1<p-1$ assumed in 2.5 implies that this character is non trivial. Let us then recall that the representation of degree one on $\bar{\mathbb{Q}}_p$ of $Gal(\bar{\mathbb{Q}}/M)$ given by $\hat{\mu}' = (\mu\hat{\varepsilon}')$ induces an irreducible representation of degree two of $Gal(\bar{\mathbb{Q}}/\mathbb{Q})$ just because $\hat{\mu}' \neq \hat{\mu}' o [\rho]$ ($\hat{\mu}' o [\rho](g) = \hat{\mu}'(g^{\rho})$): $\hat{\mu}$ is ramified at p and $\hat{\mu}' o [\rho]$ is not (in fact, this reasoning works also if we replace $\bar{\mathbb{Q}}_p$ by $\bar{\mathbb{F}}_p$ and $\hat{\mu}$ by its reduction). Now, if σ is an embedding of $\mathbb{C}(\mu\varepsilon')$ over M which fixes $K(f_{\varepsilon'})$, the representations of $Gal(\bar{\mathbb{Q}}/\mathbb{Q})$ induced from M to $\mathbb{Q}$ by $\bar{\mathbb{Q}}_p(\hat{\mu}')$ and $\bar{\mathbb{Q}}_p((\hat{\mu'^{\sigma}}))$ have the same characteristic polynomial so, being simple, they are isomorphic.

We conclude $\hat{\mu}' = (\hat{\mu'^{\sigma}})$ so $\mu' = \mu'^{\sigma}$ and σ fixes $M(\mu\varepsilon')$. Hence, $M(\mu\varepsilon') = K(f_{\varepsilon'})$.

Finally, the conductor of μ' is divisible by f because on $(\mathcal{O}/f)^{\times} \subset G_{\infty}$, $\hat{\mu}' = \hat{\mu} = \hat{\lambda}_t$ which, viewed as Dirichlet character has conductor f.

We may consequently apply the theorem 7.14 of [32] to define an abelian subvariety in $J_1(Np)$:For any ε' let $A_{f_{\varepsilon'}}$ be the abelian subvariety defined over $\mathbb{Q}$ with multiplication by $M(\mu\varepsilon')$ such that the Hecke correspondence $T(n)$ acts on it by $a(n,f_{\varepsilon'})$.

Take $A = \sum_{\varepsilon'} A_{f_{\varepsilon'}} \subset J_1(Np)$. We have an embedding of $\oplus_{\varepsilon'} M(\mu\varepsilon')$ into the $\mathbb{Q}$-algebra E of the $\mathbb{Q}$-rational endomorphisms of A. On the other hand, the characters (3.6) supply us with a surjective morphism $h_2(\Gamma_1(Np,L) \longrightarrow \otimes_{\varepsilon'} M(\mu\varepsilon')\otimes L$ inducing a surjective morphism from $R(1)$ to some local order $R(1,A)$ in $\oplus\, \iota_p(M(\mu\varepsilon'))L$. This latter algebra is direct factor in $\oplus\, M(\mu\varepsilon')\otimes L \subset E\otimes_{\mathbb{Q}} L$. We denote by $\mathfrak{M}_1(A)$ the maximal ideal of $R(1,A)$, image of $\mathfrak{M}_1$ by the projection $R(1) \longrightarrow R(1,A)$. We may consider

$V = (A[p^{\infty}]\otimes \mathcal{O}_L)[\mathfrak{M}_1(A)]$ as a $G_{\mathbb{Q}}$-module and we prove:

Lemma 3.11 : The $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$-module $V = (A[p^{\infty}]\otimes\mathcal{O}_L)[\mathfrak{M}_1(A)]$ is isomorphic to the representation induced from the character $\hat{\mu}$ $\mathrm{mod}.\mathfrak{P} = \hat{\lambda}\ \mathrm{mod}.\mathfrak{P} : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \ell^{\times}$.

Commentary :The residual fields of L , $\iota_p(M(\mu\varepsilon')).L$, $R(1,A)$, coincide with ℓ. Besides, it follows from this lemma that the module V is irreducible over $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ and is 2-dimensional over ℓ.

Proof : Set $G = (A[p^\infty] \otimes \mathcal{O}_L)$; this is an $\mathcal{O}_L$- module and a p-divisible group. We denote by Ta G its Tate module. We know that $Ta(G) \otimes_{\mathcal{O}_L} L$ is free of rank 2 over $E \otimes_{\mathbb{Q}} L$ [since $Ta(J_1(Np)) \otimes L$ is free of rank 2 over $h_2(\Gamma_1(Np), \mathbb{Q})$, and since G is obtained from $J_1(Np)[p^\infty] \otimes \mathcal{O}_L$ by taking the idempotent coming from the splitting of (3.6) over L]. Now, let $\mathcal{H}_A$ be the restriction of the Hecke algebra over $\mathbb{Z}$ to A ; then, $\mathcal{H}_A \otimes \mathcal{O}_L$ is the product of R(1,A) and of other local components.Let us write its unit 1 as $1 = \eta + \eta'$, η being the unit in R(1,A), and set $\mathfrak{M}_1$ for the maximal ideal of $\mathcal{H}_A \otimes \mathcal{O}_L$ corresponding to the component R(1,A),i.e. $\mathfrak{M}_1 = \mathfrak{M}_1(A) \times \eta'(\mathcal{H}_A \otimes \mathcal{O}_L)$;we have $\eta.G = G[\mathfrak{M}_1^\infty]$ so that $G[\mathfrak{M}_1^\infty]$ is a p-divisible group. By definition, we have $V = G[\mathfrak{M}_1]$. Let us prove that $G[\mathfrak{M}_1]$ is a 2-dimensional k-vector space. From the remarks above, it is first obvious that $\eta.Ta(G) \otimes L$ is free of rank 2 over $R(1,A) \otimes L = \bigoplus_{\varepsilon'} t_p(M(\mu\varepsilon')).L$ .Set $L_{\varepsilon'} = t_p(M(\mu\varepsilon')).L$. Then, for any character ε' of the p-part of G_1, we can consider the unit element $\eta_{\varepsilon'}$ of $L_{\varepsilon'}$; so that $\eta = \sum_{\varepsilon'} \eta_{\varepsilon'}$ and $\eta_{\varepsilon'}.\eta_{\varepsilon''} = \delta_{\varepsilon',\varepsilon''}.\eta_{\varepsilon'}$ (Kronecker symbol). For any ε', put $G_{\varepsilon'} = \eta_{\varepsilon'}.G = \eta_{\varepsilon'}.G[\mathfrak{M}_1^\infty]$ and set $\mathfrak{P}_{\varepsilon'}$ for the maximal ideal in $L_{\varepsilon'}$. The following facts hold:

1)The order generated over $\mathcal{O}_L$ by the values of $\mu\varepsilon'$ is the maximal order $\mathcal{O}_{L_{\varepsilon'}}$ of $L_{\varepsilon'}$.

2) $G[\mathfrak{M}_1] = G_{\varepsilon'}[\mathfrak{P}_{\varepsilon'}]$ and $G_{\varepsilon'}$ is an $\mathcal{O}_{L_{\varepsilon'}}$-divisible group so that

$G_{\varepsilon'}[\mathfrak{P}_{\varepsilon'}]$ is free of rank 2 over $\mathfrak{k}$.

For the assertion 1, remark that $G_\infty = W \times G_t$ and $\hat{\mu}_t = \hat{\lambda}_t$ so $L_{\varepsilon'}$ = L(values of ε') and $\mathcal{O}_{L_{\varepsilon'}} = \mathcal{O}_L$[values of ε'] = $\mathcal{O}_L$[values of $\mu\varepsilon'$]

For the assertion 2, it suffices to notice that $\mathfrak{M}_1(A)$ projects onto $\mathfrak{P}_{\varepsilon'}$ via the character $R(1,A) \to \mathcal{O}_{L_{\varepsilon'}}$ given by $\theta(\hat{\mu}\hat{\varepsilon}')$; this yields the equality $G[\mathfrak{M}_1] = G_{\varepsilon'}[\mathfrak{P}_{\varepsilon'}]$ and the last assertion results from the exact sequence, valid for any $\mathcal{O}_{L_{\varepsilon'}}$-divisible group $\mathcal{G}$:

$$0 \to \mathfrak{P}_{\varepsilon'}.Ta(\mathcal{G}) \to Ta(\mathcal{G}) \to \mathcal{G}[\mathfrak{P}_{\varepsilon'}] \to 0$$

We may apply it because since $\mathcal{O}_{L_{\varepsilon'}}$ is a discrete valuation ring , the lattice $Ta(G_{\varepsilon'})$ in the 2-dimensional vector space $L_{\varepsilon'} \otimes Ta(G_{\varepsilon'})$ is free of rank 2 over $\mathcal{O}_{L_{\varepsilon'}}$, so $G_{\varepsilon'}$ is $\mathcal{O}_{L_{\varepsilon'}}$-divisible.

Now, by an easy calculation, one checks that for any rational prime ℓ, $\ell \nmid Np$, the Frobenius automorphism acting on our 2-dimensional representation $V = G_{\varepsilon'}[\mathfrak{P}_{\varepsilon'}]$ (independent of the character ε' as above by the foregoing) has characteristic polynomial $X^2 - T(\ell)X + \ell\langle\ell\rangle_2$ mod $\mathfrak{M}_1$ which coincides with the characteristic polynomial of $Frob_\ell$ acting on the induced representation of $\hat{\lambda}$ mod.$\mathfrak{P}_{\varepsilon'}$ = $\hat{\mu}$ mod.$\mathfrak{P}_{\varepsilon'}$: $Gal(\bar{\mathbb{Q}}/M) \to \mathfrak{k}^\times$ of M to $\mathbb{Q}$. By the Brauer-Nesbitt theorem, it implies the isomorphism of these 2 representations taking into account the remark $\hat{\lambda} \not\equiv \hat{\lambda}o[\rho]$ mod.$\mathfrak{P}$ as already mentioned.

Corollary :The component R attached to χ is Gorenstein.

Proof:Apply criterion 3.6. This is allowed since our integer

a mod.p-1 is $\nu+1 \not\equiv 1,2$ mod.p-1.

In the next paragraph, we will explain precisely the number-theoretic situation we want to deal with and give the main result concerning it.

4. The anticyclotomic $\mathbb{Z}_p$-extension and its Iwasawa Theory.

In this paragraph, the notations concerning the imaginary quadratic field M and the related datas are still in force. So are the hypotheses 2.5. In particular, p splits in M.
Let $\tilde{K}$ be the ray-class field of M of conductor p.Nf, K the Ringklassenkörper of M for the order $\mathbb{Z}+p.Nf.\mathcal{O}$. We recall that there are two natural $\mathbb{Z}_p$-extensions associated with an imaginary quadratic field, namely, the cyclotomic $\mathbb{Z}_p$-extension M_∞^+/M, which is the union of the fields $\mathbb{Q}_r.M$ ($\mathbb{Q}_r/\mathbb{Q}$ being the p-part of $\mathbb{Q}(\zeta_{p^{r+1}})/\mathbb{Q}$), r=1,2,.., and the anticyclotomic $\mathbb{Z}_p$-extension M_∞^-, which is the union of the p-part of the Ringklassenkörpern of M for the order $\mathbb{Z}+p^{r+1}.\mathcal{O}$, r=1,2,... Furthermore, since we supposed that p is splitted in M into p and p^ρ, there are two other natural $\mathbb{Z}_p$-extensions, namely $M_\infty(p)$ (resp. $M_\infty(p^\rho)$) the unique $\mathbb{Z}_p$-extension unramified outside p (resp. p^ρ). One can easily see that the compositum of any two of those four $\mathbb{Z}_p$-extensions coincide with the unique $\mathbb{Z}_p^2$-extension $\tilde{M}_\infty$ of M. We put $\tilde{K}_\infty = \tilde{K}.\tilde{M}_\infty$, $\tilde{K}_\infty^+ = \tilde{K}.M_\infty^+$, $\tilde{K}_\infty^- = \tilde{K}.M_\infty^-$, $K_\infty^- = K.M_\infty^-$, so that $\tilde{K}_\infty/\tilde{K}$ is the lifting to $\tilde{K}$ of the $\mathbb{Z}_p^2$-extension of M, $\tilde{K}_\infty^+/\tilde{K}$ is the cyclotomic $\mathbb{Z}_p$-extension of $\tilde{K}$ and $\tilde{K}_\infty^-/\tilde{K}$, resp. K_∞^-/K is the so-called anticyclotomic $\mathbb{Z}_p$-extension of $\tilde{K}$ resp.K. In fact, K_∞^- is the union of the Rinklassenkörpern of M

of conductor $p^r.Nf$ for $r=1,2,\ldots$ Now, let S_p be the set of primes in K above p, and S the subset in S_p consisting of primes above p. So, we have $S_p = S \cup S^\rho$. Consider the maximal abelian p-extension M_∞^S of K_∞^- unramified outside S. We note $X_\infty^S = \mathrm{Gal}(M_\infty^S/K_\infty^-)$. As in the introduction, we can consider this compact $\mathbb{Z}_p$-module as a $\mathbb{Z}_p[[W^-]]$-module, where $W^- \subset \mathrm{Gal}(K_\infty^-/M)$ is a direct factor isomorphic to $\mathbb{Z}_p$ in $\mathrm{Gal}(K_\infty^-/M)$, acting on X_∞^S by conjugation. If $\Gamma^- = \mathrm{Gal}(K_\infty^-/K)$, we have $(W^-:\Gamma^-) = p^d$ as we can check, using $p \nmid 6N\varphi(N)$. So, $\mathcal{O}_L[[W^-]] \simeq \mathcal{O}_L[[X]] = \mathcal{I}$. We will fix later a good choice for such an isomorphism, depending on the fixed group W we specified in §2.

Next, by using the datum of $\hat{\lambda}$, we may define a character κ of $\Delta = \mathrm{Gal}(K/M)$ by:

(4.1) $\kappa : \Delta \to \bar{k}^x$, $\kappa(\sigma) = \mathrm{Teich.}(\hat{\lambda}(\sigma)/\hat{\lambda}\circ[\rho](\sigma) \bmod \mathfrak{P})$,

where $\hat{\lambda}$ is viewed as Galois character thanks to the Artin reciprocity law

(4.2) $\hat{\lambda}: \mathrm{Gal}(\bar{\mathbb{Q}}/M) \to \mathrm{Gal}(M(\mathfrak{f}p^\infty)/M) \simeq G_\infty \xrightarrow{\hat{\lambda}} \mathcal{O}_L^x$

and $k^x \xrightarrow{\text{Teich}} \mathcal{O}_L^x$ is the Teichmüller lifting. The first map is just the restriction of automorphisms to the union of class fields of M of conductors $\mathfrak{f}p^r$, $r=1,2,\ldots$, the isomorphism is given by Artin reciprocity. As in the previous paragraph, $\hat{\lambda}\circ[\rho](\sigma) = \hat{\lambda}(\rho\sigma\rho)$.

We are concerned with the $\mathcal{O}_L[[W^-]]$-module $X_\infty^S(\kappa) = \{x \in X_\infty^S \otimes \mathcal{O}_L;\ x^\delta = \kappa(\delta).x\}$. Be careful that Δ doesn't act itself on X_∞^S because its order may be divisible by p, but its non-p-part, say Δ', does. The point is that we are only concerned with characters of Δ'. Incidentally, note that W^- and Δ' are direct factors in

$Gal(K_\infty^-/M)$.

Let us explain more concretely what is the κ-part of X_∞^S under some simplifying hypotheses. So, suppose that the class number of M is one and take an integer i modulo p-1, e.i$\not\equiv$0,1 mod.p-1. ($\#\mathcal{O}^X$ = 2.e). Then the Ringklassengruppe R_p of the order $\mathcal{O}(p)=\mathbb{Z}+p.\mathcal{O}$ is inserted in the following exact sequence:

$$0 \to \mathcal{O}^X.\mathbb{F}_p^X \to (\mathcal{O}/p\mathcal{O})^X \to R_p \to 0$$

where the first map is induced by the inclusions $\mathcal{O}^X\subset\mathcal{O}$ and $\mathbb{Z}\subset\mathcal{O}$ reduced mod.p, and the second one sends $\alpha\in\mathcal{O}$, prime to p, to the class of the ideal $\alpha.\mathcal{O}\cap\mathcal{O}_p$. Besides, the Artin reciprocity map yields a canonical ismorphism $R_p \simeq \Delta$. Since p splits in M , we have $(\mathcal{O}/p\mathcal{O})^X = \mathbb{F}_p^X \times \mathbb{F}_p^X$, the inclusion $\mathbb{F}_p^X \subset (\mathcal{O}/p\mathcal{O})^X$ becoming the diagonal map. Consider the character

$$(\mathcal{O}/p\mathcal{O})^X \to \mathbb{F}_p^X : (x,y) \to (x/y)^e$$

it factorises through R_p, hence defines a character of Δ whose lifting to $\mathbb{Z}_p^X$ we call the basic anticyclotomic character κ_0. It is the analogous of the basic cyclotomic character ω in the cyclotomic case. It establishes an isomorphism between Δ and $(\mathbb{F}_p^X)^e$ (subgroup of e-th powers in $\mathbb{F}_p^X$). On the other hand, if we make the assumption that i is even (just for simplicity), the datum of i mod.p-1 provides us with a Grössencharacter λ of type $(\nu,0)$ and conductor 1 given by $\lambda((\alpha))=\alpha^\nu$, $\nu \equiv$ e.i mod.p-1, $\nu<$p-1, so that the hypotheses 2.5 are fulfilled. The character κ defined above from λ is nothing but κ_0^i; hence, we are looking to $X_\infty^S(\kappa_0^i)$, the κ_0^i-part of the anticyclotomic Iwasawa module X_∞^S.

In this setting, the analogy with the cyclotomic situation

presented in the introduction is clear.

Let us come back to the more general case, that is hypotheses 2.5 only. Since the group Δ may have a p-part, but we are interested in characters factorising through the Teichmüller character of L, i.e. of order prime to p; we introduce the non-p-part of Δ we denote by Δ'. We prove now an important proposition for our purposes. It is due to R. Greenberg and B. Perrin-Riou (cf.[25]).

Proposition 4.1:The $\mathbb{Z}_p[[\Gamma^-]]$-module X_∞^S is finitely generated and torsion (we use the catch-word Λ-finite to shorten this). In particular, for any ξ in $\mathrm{Hom}(\Delta,\bar{\mathbb{Q}}_p^{\times})$, the (Teich.o$\xi$)-part of X_∞^S is $\mathcal{O}_L[[\Gamma^-]]$-finite. In other words, for all characters ξ' in $\mathrm{Hom}(\Delta',\mathcal{O}_L^{\times})$, $X_\infty^S(\xi')$ is $\mathcal{O}_L[[\Gamma^-]]$-finite.

Proof: Let M_r^S resp. X_r^S the analogous of M_∞^S resp. X_∞^S for the field K_r^-, defined as the subfield of K_∞^- fixed by $(\Gamma^-)^{p^{r-1}}$; let $U_{r,S}$ be the group of semilocal units above p (note that p is almost totally ramified in M_∞^-/M, so that the number of places in K_r^- above S is bounded in r). Let also E_r be the group of global units in K_r^-; then, global class field theory supplies us with the exact sequence :

$$0 \to (U_{r,S}/\bar{E}_r)(p) \to X_r^S \to X_r^{\phi} \to 0$$

where for any abelian profinite group G, G(p) denotes its pro-p-Sylow, and $\bar{E}_r$ is the closure of E_r diagonally embedded into $U_{r,S}$.

Now, since K_r^-/M is abelian, Brumer's theorem applies, so that Leopoldt's conjecture is true : $\mathrm{rank}_{\mathbb{Z}_p}\bar{E}_r = [K_r^-:M]-1$. Besides,

the Galois module $U_{r,S}\otimes\mathbb{Q}_p$ is isomorphic to $\mathbb{Q}_p[\mathrm{Gal}(K_r^-/M)]$ and one deduces easily from Dirichlet's units theorem that $E_r\otimes\mathbb{Q}_p$ is isomorphic to the augmentation representation of $\mathrm{Gal}(K_r^-/M)$. Hence, $(U_{r,S}/\bar{E}_r)\otimes\mathbb{Q}_p$ is isomorphic to the trivial Galois module $\mathbb{Q}_p$. So, for any non trivial character ξ' of Δ', we see that $X_r^S(\xi')$ is finite for any $r>0$. But in any case, we see that the $\mathbb{Z}_p$-module X_r^S is of rank at most one.

We fix arbitrarily a topological generator γ^- of Γ^- so that we can identify $\mathbb{Z}_p[[\Gamma^-]]$ with Λ (a better choice for γ^- will be specified later but we don't use it right now). Let us consider the classical Iwasawa polynomials $\omega_r(T)=(1+T)^{p^{r-1}}-1$, $r>0$, and $\omega_{r,r'}(T)=\omega_r(T)/\omega_{r'}(T)$, $r\geq r'>0$. We recall the formula comparing $X_\infty^S/\omega_r.X_\infty^S$ and X_r^S. During the following of the proof, we drop the cumbersome exponent S in X_∞^S and M_∞^S. Put $\mathfrak{G}_r=\mathrm{Gal}(M_\infty/K_r^-)$; $I_{r,\tilde{v}}\subset\mathfrak{G}_r$ denotes the inertia subgroup at some place $\tilde{v}$ of M_∞ above $S_p\backslash S$ (i.e. above p^ρ). Let c be the smallest integer such that any place in K_c^- above p^ρ is totally ramified in K_∞^-. Then, for any $r\geq c$, the restriction $\mathfrak{G}_r\to\Gamma_r^-$ induces an isomorphism $I_{r,\tilde{v}}\simeq\Gamma_r^-$. From that, it follows that $\mathfrak{G}_r$ is semi-direct product of $I_{r,\tilde{v}}$ and X_∞. We denote by $\sigma_{\tilde{v}}$ the element of $I_{c,\tilde{v}}$ corresponding to γ^-. Let $v_1,\ldots,v_s$ the primes in K_c^- above p^ρ. Fix a prime $\tilde{v}_i$ in M_∞ above v_i, $i=1,\ldots,s$; we may write $\sigma_{\tilde{v}_i}=\sigma_{\tilde{v}_1}a_i$ for some a_i in X_∞. Remark that if we take two primes $\tilde{v}_i$ and $\tilde{v}_i'$ in M_∞ above the same prime $v_i\in\{v_1,\ldots,v_s\}$, the elements a_i and a_i' differ only by an

element in $\omega_c.X_\infty$; in fact, there is $x \in X_\infty$ such that $\sigma_{\tilde{v}_i'} = x\sigma_{\tilde{v}_i}x^{-1}$ hence $\sigma_{\tilde{v}_1}.a_i = x\sigma_{\tilde{v}_1}x^{-1}a_i' = \sigma_{\tilde{v}_1}.(\sigma_{v_1}^{-1},x).a_i'$ and the commutator $(\sigma_{v_1}^{-1},x)$ belongs to $\omega_c.X_\infty$. Finally, consider the normal subgroup $\mathcal{I}_r$ in $\mathfrak{G}_r$ generated by the $I_{r,\tilde{v}_i}$'s . Then, it is easy to see that X_r identifies with $\mathfrak{G}_r/(\mathfrak{G}_r,\mathfrak{G}_r).\mathcal{I}_r$. Besides, modulo $(\mathfrak{G}_r,\mathfrak{G}_r) = \omega_r.X_\infty$, we have $\mathcal{I}_r \equiv I_{r,\tilde{v}_1}.\omega_{r,c}.(a_2,\ldots,a_s)$ because $\sigma_{\tilde{v}_i}^{p^{r-e}} = \sigma_{\tilde{v}_1}^{p^{r-e}}.\omega_{r,c}.a_i$, for all $r \geq c$. Henceforth, we get $X_r = X_\infty/\omega_r.X_\infty + \omega_{r,c}.(a_2,\ldots,a_s)$ which can be written, by putting $Y_\infty = \omega_c.X_\infty + (a_2,\ldots,a_s)$, $X_r = X_\infty/\omega_{r,c}.Y_\infty$. Let us notice that $\omega_{r,c}.Y_\infty/\omega_r.X_\infty$ is a $\mathbb{Z}_p$-module of rank $\leq p^c.(s-1)$ for all $r \geq c$, because Γ_c^- acts trivially on $Y_\infty/\omega_c.X_\infty$ and $\omega_{r,c}.Y_\infty/\omega_r.Y_\infty \to Y_\infty/\omega_c.X_\infty$ has pseudo-null kernel (i.e. these two $\mathbb{Z}_p$-modules have the same $\mathbb{Z}_p$-rank). From this, it results immediately that X_∞ is finitely generated and more precisely, we have the exact sequence:

$$0 \to \omega_{r,c}.Y_\infty/\omega_r.X_\infty \to X_\infty/\omega_r.X_\infty \to X_r \to 0$$

We get from this that the $\mathbb{Z}_p$-rank of $X_\infty/\omega_r.X_\infty$ is bounded in r (by the constant $p^c.(s-1)+1$). So, we conclude that X_∞ is Λ-torsion. This implies of course the finiteness over Λ_L of any of its ξ'-part.

Remark : If we suppose that p doesn't divide the class-number of M, since $p \nmid N\varphi(N)$, we see that p doesn't divide $\#\Delta$ and all the primes v_i in the proof above ramify totally in K_∞^- ; this simplifies the proof above because then $Y_\infty = X_\infty$ and $X_r =$

$X_\infty/\omega_r.X_\infty$.

Corollary 4.2: $X_\infty^S(\kappa)$ is a torsion $\mathcal{O}_L[[W^-]]$-module.

We now fix a good topological generator of W^-: let $\tilde{K}(p^\infty)$ be the compositum of $\tilde{K}$ and $M(\mathfrak{f}p^\infty)$; note that the restriction map gives an isomorphism on the p-parts of $Gal(\tilde{K}(p^\infty)/K) \to Gal(M(\mathfrak{f}p^\infty)/M)$ so that the group W fixed in §2 as direct factor isomorphic to $\mathbb{Z}_p$ in $G_\infty \simeq Gal(M(\mathfrak{f}p^\infty)/M)$ can be lifted to $Gal(\tilde{K}(p^\infty)/M)$. Let w be the unique element in W such that $\hat{\lambda}_0(w)^{p^d} = u = 1+Np$. Then take w_0 to be the unique element in the p-part of $Gal(\tilde{K}_\infty/M)$ such that $w_0^p = w_0^{-1}$ and $w_0|_{\tilde{K}(p^\infty)} = w^{1/2}$. We set $w^- = w_0|_{K_\infty^-}$; from now on, this w^- will not be changed, it fixes identifications

$$\mathcal{O}_L[[W^-]] \simeq \mathcal{O}_L[[X]],\ \mathbb{Z}_p[[\Gamma^-]] \simeq \mathbb{Z}_p[[T]],\ \text{and}\ \mathcal{O}_L[[\Gamma^-]] \simeq \Lambda_L.$$

Because of corollary 4.2, we may consider the characteristic power series $f(X)= f_{(\lambda,\iota_p)}(X) \in \mathcal{O}_L[[X]]$ attached to $X_\infty^S(\kappa)$. On the other hand, recall that the Congruence Module is a torsion I-module ($\simeq R_1/c_1$, with $R_1=I$ as noticed in §2). Hence it has a characteristic power series in I we denoted by $H_{(\lambda,\iota_p)}(X)$ in §2.

We abbreviate $\hat{\lambda}_0(w)$ by v. This is a p^d-th root of u in L.

The main result of these notes reads:

Theorem 4.3 : The divisibility $H_{(\lambda,\iota_p)}(X) \mid f_{(\lambda,\iota_p)}(v^{-1}(1+X)-1)$ holds in I, provided the hypotheses 2.5 are assumed.

Remark: 1) Theo.4.3 is a slight improvement compared to theorem 3. 3 in [35] because we don't suppose here that p doesn't divide the class number of M. This is important because of a

possible vast generalisation of it replacing M by $M(\zeta_{p^r})$ for r=1,... so that the p-class-number of those fields tends towards infinity in general. For more explanations about this possible generalisation, look at the last paragraph of [13].

3) From this theorem, it is easy to recover the Kummer's criterion given as corollary of theorem 0.1 of [9], provided one knows the weak interpolation theorem satisfied by the series $H_{(\lambda, t_p)}(X)$(§10 of [11] when d=0, and [39], §4 in general), for details about this, see §3 of [35].

4) Some numerical examples for the theorem not to be empty arise from Maeda's table quoted in §8 of [7].

5) In fact, this theorem is only a corollary of the existence of a Λ_L-linear surjective morphism from (a twist of) $X_\infty^S(\kappa)$ to the module of differentials of the character χ: $R \to \mathcal{O}_L[[X]]$. This module is defined in [13] and compared to the congruence module, the conjecture being that the Fitting ideals over Λ_L of those two modules are equal, provided R is Gorenstein. In fact, this is an important point in this work to prove <u>one</u> inclusion (the one we need of course). This is explained in §9 below. Incidentally, it is interesting to notice that this inclusion of Fitting ideals doesn't require the Gorenstein-ness of R to be true. The other one must use it since there are some counter-example by H. Bass (mentioned in [13]) to the equality for non-Gorenstein rings.

The next topic, of course is to construct the map mentioned above from Iwasawa module to differential module. This

involves some results on the arithmetic of modular curves. In particular, in the next paragraph, we will explain a little more the result alluded to in 3.9.

5. The Λ-divisible group attached to the component R and the Λ-linear map from (twisted) $X_\infty^S(\kappa)$ to the module of differentials.

For any $r>0$, we consider the curve $X_1(Np^r)_{/\mathbb{Q}}$ defined as the projective and smooth model of the fixed part of the field of $\Gamma_1(Np^r)$-modular functions for the action of $\mathrm{Aut}(\mathbb{C})$ on the q-expansion at the infinity cusp. This is a geometrically connected curve. Let φ denote the canonical holomorphic map from the upper half plane $\mathfrak{h}$ to the set of complex points of $X_1(Np^r)$ endowed with its natural analytic structure. Recall that the group $(\mathbb{Z}/Np^r\mathbb{Z})^\times/\{\pm 1\}$ acts faithfully on $X_1(Np^r)$ by $\mathbb{Q}$-rational automorphisms. We denote by $a \to \langle a\rangle_2$ this action ("diamonds of weight 2", this is compatible with the terminology of §1 as we shall see). It is caracterised by the formula: for a prime to Np and $\sigma_a \in SL_2(\mathbb{Z})$, $\sigma_a \equiv \begin{pmatrix} a^{-1} & \\ & a \end{pmatrix}$ mod. Np^r, we have for all z in $\mathfrak{h}$

$$\langle a\rangle_2 \varphi(z) = \varphi(\sigma_a z).$$

For all prime number ℓ, we also have the Hecke correspondence $T(\ell)$ on $X_1(Np^r)$, rational over $\mathbb{Q}$, caracterised by:

$$T(\ell)\varphi(z) = \begin{cases} \sum_{i=1}^{\ell-1} \varphi\left(\frac{z+i}{\ell}\right) + \varphi(\ell z) & \text{if } \ell \nmid Np \\ \sum_{i=1}^{\ell-1} \varphi\left(\frac{z+i}{\ell}\right) & \text{if } \ell \mid Np \end{cases}$$

In a notation compatible with §1, we may still denote by $h_{2,r}(\mathbb{Z})$ the $\mathbb{Z}$-algebra generated by the $\langle a\rangle_2$ and the $T(\ell)$'s acting by pull-back of divisor classes on the jacobian $J_1(Np^r)_{/\mathbb{Q}}$ of $X_1(Np^r)_{/\mathbb{Q}}$. This is easy to check, or see prop.7.1 in [32]. Note that on the tangent space $S_2(\Gamma_1(Np^r))$ of $J_1(Np^r)$, $\langle a\rangle_2$ acts by $f \to f|_2\sigma_a$.

We now consider the p-divisible group $J_1(Np^r)[p^\infty]_{/\mathbb{Q}}$ of the jacobian. We endow it with the following action of $G_{\mathbb{Q}}=\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$. Take the morphism :

$$G_{\mathbb{Q}} \to \mathrm{Gal}(\mathbb{Q}(\xi_{Np^r})/\mathbb{Q}) \simeq (\mathbb{Z}/Np^r\mathbb{Z})^\times \to h_{2,r}(\mathbb{Z}_p)$$

denoted by $\sigma \to \langle\sigma\rangle_2$; then, we set, for $P\in J_1(Np^r)[p^\infty](\bar{\mathbb{Q}})$:

$$\sigma_{\mathrm{Pic}}P = \langle\sigma\rangle_2\, P^\sigma$$

where $P \to P^\sigma$ is the usual action of $G_{\mathbb{Q}}$ on algebraic points.

Note: The importance of this twisted action has already appeared in §3 (proof of prop. 3.7) because since the Hecke correspondences act contravariantly, in order to get the usual Eichler-Shimura relations, we have to twist the Galois action. Now, it is clear that the $\mathcal{O}_L$-divisible group

$$(5.1) \qquad \mathcal{O}_L \otimes J_1(Np^r)[p^\infty](\bar{\mathbb{Q}})$$

is an $h_{2,r}(\mathcal{O}_L)$- and $G_{\mathbb{Q}}$- module, and these actions commute. Let η_R be the unit element of our local component R; thanks to th. 1.8, we may apply this idempotent to the group (5.1). By this way, we get an R(r) - and $G_{\mathbb{Q}}$- module :

$$(5.2) \qquad J_r(R) = \eta_R.(\mathcal{O}_L \otimes J_1(Np^r)[p^\infty](\bar{\mathbb{Q}}))$$

As in Prop.3.4 , we put $R(r) = R/\omega_{2,r}R$, for all $r>0$.

For $r'\geq r>0$, we have a $\mathbb{Q}$-rational covering $X_1(Np^{r'}) \to X_1(Np^r)$ coming from the inclusion $\Gamma_1(Np^r) \subset \Gamma_1(Np^{r'})$. It provides a

morphism with finite kernel $J_1(Np^r) \to J_1(Np^{r'})$ compatible with the actions of $h_{2,r}(\mathbb{Z}_p)$ and $h_{2,r'}(\mathbb{Z}_p)$. We set:

$$(5.3) \qquad J(R) = \varinjlim_r J_r(R)$$

for the transition maps deduced from the above.

In [11], Hida proved the following theorem (theorem 3.1 of [11]):

Theorem 5.1 : The R-linear morphisms $J_r(R) \to J_{r'}(R)$ are injective and

$$J(R)[\omega_{2,r}] = J_r(R)$$

Next, we want to determine the structure of R-module of J(R). This is done in theorem 4.4 of [34], but we will here explain the idea.

First, to deal with true algebro-geometric objects, we look at the component $\underline{R}$ of $h^{ord}(Np^\infty, \mathbb{Z}_p)$ such that $R = \underline{R} \otimes \mathcal{O}_L$. To $\underline{R}$, we may similarly attach $J_r(\underline{R})$ which is contained in the $J_1(Np^r)$ for all $r>0$. We still have $\underline{R} \subset h^{ord}(a)$ $(a=\nu+1)$ and $\underline{R}$ is Gorenstein because $\underline{R} \otimes \mathcal{O}_L$ is.

Fact 1: Because of $a \neq 2$, there is an abelian subvariety A_r in $J_1(Np^r)$ containing $J_r(\underline{R})$ such that:

(i) A_r is defined over $\mathbb{Q}$

(ii) A_r is stable under $h_{2,r}(\mathbb{Z})$,

(iii) A_r has good reduction at p over $\mathbb{Q}(\xi_{p^r})$.

The proof is detailed in §1 of [34]; the formula for A_r is

$$(5.4) \qquad A_r = \sum A_f|[t]$$

where f runs in the set of primitive newforms of level C(f) divisible by p, with Nebentypus of conductor at p equal to the

p-part of C(f), and t running in the set of divisors of N/(N,C). The map [t] is deduced by Picard functoriality from the $\mathbb{Q}$-rational covering $X_1(Np^r) \to X_1(C(f))$ coming from

$$\begin{pmatrix} t & \\ & 1 \end{pmatrix} . \Gamma_1(Np^r) . \begin{pmatrix} t & \\ & 1 \end{pmatrix}^{-1} \subset \Gamma_1(C(f))$$

$$[t] : J_1(C(f)) \to J_1(Np^r),$$

From fact 1, we see that $J_r(\underline{R})$ is also a direct factor in the ordinary part of the p-divisible group $A_r[p^\infty]_{/\mathbb{Q}}$.

Let $\mathcal{O}_r$ be the ring of integers in $\mathbb{Q}_p(\zeta_{p^r})$, we may consider the schematic closure of $J_1(\underline{R})$ inside the abelian scheme $A_{r/\mathcal{O}_r}$. We thus obtain a p-divisible group over the complete discrete valuation ring $\mathcal{O}_r$. Taking the connected-etale unscrewing of $A_{r/\mathcal{O}_r}$, we obtain an exact sequence of p-divisible groups

$$0 \to \mathcal{G}_{r/\mathcal{O}_r} \to A_r[p^\infty]_{/\mathcal{O}_r} \to \mathcal{E}_{r/\mathcal{O}_r} \to 0$$

and by applying to the p-divisible groups $\mathcal{G}_{r/\mathcal{O}_r}$ and $\mathcal{E}_{r/\mathcal{O}_r}$ the idempotent of End A_r corresponding to $\underline{R}(r)$, we define the connected component $C_{r/\mathcal{O}_r}$ of $J_r(\underline{R})_{/\mathcal{O}_r}$ and its etale component $E_{r/\mathcal{O}_r}$, thus constructing the following exact sequence :

$$(5.5) \qquad 0 \to C_{r/\mathcal{O}_r} \to J_r(\underline{R})_{/\mathcal{O}_r} \to E_{r/\mathcal{O}_r} \to 0$$

The crucial result about this exact sequence is

Fact 2: For $a \neq 1,2$, the exact sequence of $\underline{R}$-modules given by the geometric points of (5.5) splits for each $r>0$. Furthermore, the maps $J_r(\underline{R}) \to J_{r'}(\underline{R})$ for $r'>r>0$ induce $C_r \to C_{r'}$ and $E_r \to E_{r'}$, and the splittings are compatible with these maps, so that we get:

$J(\underline{R}) \simeq C \oplus E$ as $\underline{R}$-modules, where $C = \varinjlim_r C_r$, $E = \varinjlim_r E_r$

The point to verify this statement is to determine the Galois action on C and E. Indeed, the decomposition group of $\bar{\mathbb{Q}}_p$ over $\mathbb{Q}_p(\xi_{p^r})$ acts on C_r and E_r but through a p-group; this doesn't imply any splitting. Fortunately, the full inertia group I_p of $\bar{\mathbb{Q}}_p/\mathbb{Q}_p$ acts on C_r and E_r by what is called the geometric action of inertia. The reason for that is simply that I_p acts on $J_r(\underline{R})$ hence on C_r and E_r by functoriality of connected and etale component. Next, one has to determine this action. On the etale part, one finds it is trivial because the inclusion $A_r \subset J_1(Np^r)$ induces an isogeny from the ordinary part of the special fiber of $A_r[p^\infty]$ to $j_r^\infty[p^\infty]^{et}$, where j_r^∞ is the jacobian of the curve C_r^∞ which is the normalisation of the irreducible component containing the infinity cusp in the minimal regular model $X_1(Np^r)^{\#}_{/\mathcal{O}_r}$ of $X_1(Np^r)_{/\mathcal{O}_r}$. For the details, see [34] §3, and [21] chap.2, §8).The triviality of the action of I_p on C_r^∞ (hence on j_r^∞) results then from the $\mathbb{Q}$-rationality of the cusp ∞ : I_p acts only by permutation on the set of irreducible components of $X_1(Np^r)^{\#}\otimes\mathbb{F}_p$ so fixes C_r^∞ . Then, we deduce that the action on the connected component C_r is given for any integer b prime to Np and any P in C_r by:

$$\left(\frac{\mathbb{Q}(\xi_{Np^\infty})/\mathbb{Q}}{b}\right)_{Pic}.P = \langle b\rangle_2.b.P$$

This is an easy corollary from the Cartier duality between C_r and E_r coming itself from [21], chap.3 prop. 2 and 3 (see theo. 3.1 of [34] for further explanations).

From this rather delicate analysis, we conclude that $Gal(\bar{\mathbb{Q}}_p/\mathbb{Q}_p)$

acts through $H = Gal(\mathbb{Q}_p(\zeta_{Np^\infty})/\mathbb{Q}_p)$ on E_r and C_r and the subgroup H_0 of H fixing ζ_N and the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}$ acts by 1 on E_r and by ω^{a-1} on C_r. Now, we use that $a \neq 1$ to obtain the splitting of the sequence over $\underline{R}$. The compatibility with the transition maps is easy to check.

On the other hand, the control theorem 5.1 combined to the above theorem 5.2 supplies us with the control of the connected and etale parts of $J(\underline{R})$:

Fact 3: For all $r>0$, $C[\omega_{2,r}] = C_r$, $E[\omega_{2,r}] = E_r$.

But, as already mentioned in §3 (theo.3.9), a previous result by Hida ([9] prop.3.1) gives the structure of C_1 and E_1 as $\underline{R}_1$-modules: $C_1 = \underline{R}(1) \otimes \mathbb{T}_p$, $E_1 = Hom(\underline{R}(1), \mathbb{T}_p)$. The last tool we need is the Pontryagin duality. For any $\underline{R}$- and $G_{\mathbb{Q}}$- module $\mathcal{M}$, we put on its Pontryagin dual $\mathcal{M}^*$ the following structures of $\underline{R}$- and $G_{\mathbb{Q}}$-module: for $r \in \underline{R}$, $\sigma \in G_{\mathbb{Q}}$, $x \in \mathcal{M}$, $x^* \in \mathcal{M}^*$,

$$\langle x, r.x^* \rangle = \langle r.x, x^* \rangle, \quad \langle \sigma x, \sigma x^* \rangle = \langle x, x^* \rangle.$$

We can then convert Fact 3 into:

$$C^*/\omega_{2,r}.C^* = C_r^* , \quad E^*/\omega_{2,r}.E^* = E_r^*$$

By applying this to $\omega_{2,1}$, and by computing Λ-ranks, we obtain:

Theorem 5.2: For all $r>0$, the connected-etale sequence (5.5) is splitted: $J_r(\underline{R}) = C_r \oplus E_r$, and $C_r \simeq \underline{R}(r) \otimes \mathbb{T}_p$, $E_r \simeq Hom(\underline{R}(r), \mathbb{T}_p)$. and $J(\underline{R}) = C \oplus E$, $C^* \simeq Hom_{\Lambda}(\underline{R}, \Lambda)$, $E^* \simeq \underline{R}$.

If we now remind ourselves of the link between $\underline{R}$ and R, we draw from theorem 5.2 the corollary:

Corollary 5.3: There is an R-linear isomorphism

$$J(R)^* \simeq R \oplus Hom_{\Lambda_L}(R, \Lambda_L)$$

but, since we proved that R is Gorenstein, we may strengthen this into:

$J(R)^*$ is free of rank two over R.

This will be of course crucial for the following construction of our map from the Iwasawa module to the module of differentials. So let us proceed now to this construction.

Notation 5.4: We denote by η_i i=1,2 the idempotents in $R\otimes\mathcal{L}_L$ corresponding to the decomposition

$$(1.11) \qquad R\otimes\mathcal{L}_L \simeq \mathcal{X} \oplus \mathcal{B}$$

where the first projection is given by χ.

We set $R_1 = \mathrm{Im}\,(pr_1: R \to \mathcal{X})$, $R_2 = \mathrm{Im}\,(pr_2: R \to \mathcal{B})$, $c_2 = \mathrm{Ker}(pr_1: R \to \mathcal{X})$ and $c_1 = \mathrm{Ker}(pr_2: R \to \mathcal{B})$. Now, by theorem 5.2, $J(R)^*$ is Λ_L-free so $J(R)$ is Λ_L-divisible. This permits us to look at the following parts of $J(R)$:

Notation 5.5: We set $A = \eta_1.J(R) = J(R)[c_2]$ and $B = \eta_2.J(R) = J(R)[c_1]$. Similarly, for all r>0, we set $A_r = J_r(R)[c_2]$ and $B_r = J_r(R)[c_1]$.

Since $J_r(R)$ is contained in $J(R)$ (and equal to its $\omega_{2,r}$-torsion), these notations are meaningful.

Proposition 5.6: We have R-linear isomorphisms:

$$A^* \simeq R_1 \oplus R_1 \ , \quad B^* \simeq R_2 \oplus R_2, \quad (A \cap B)^* \simeq C_0(\mathcal{X}) \oplus C_0(\mathcal{X})$$

and similarly, for all r>0,

$$A_r^* \simeq A^* \otimes (\Lambda_L/\omega_{2,r}\Lambda_L), \quad B_r^* \simeq B^* \otimes (\Lambda_L/\omega_{2,r}\Lambda_L),$$

$$(A_r \cap B_r)^* \simeq C_0(\mathcal{X}) \otimes (\Lambda_L/\omega_{2,r}\Lambda_L).$$

In particular, the Pontryagin duals of A and B are Λ_L-torsion free hence A and B are Λ_L-divisible groups.

Proof: This is an easy exercise in Pontryagin duality, starting

with the R-bilinear pairing:

$$J(R) \times R^2 \longrightarrow \mathbb{T}_p$$

We leave it to the reader.

Corollary 5.7: We have the equality:

$$A \cap B = A[c_1] = B[c_2] ,$$

and similarly for all $r>0$: $A_r \cap B_r = A_r[c_1] = B_r[c_2]$.

Proof: Just check that the Pontryagin duals coincide by using the previous proposition.

Some words about our strategy are now in order. The corollary 5.7 is powerful because it expresses the equality of parts of radically different objects. We will see that the Λ_L-divisible group A is of Complex Multiplication type whereas B has no complex multiplications (the precise statement is given below) This is henceforth a hint that by modifying a little $B[c_2]$, we will get an interesting Galois module, whose non-splitness will in fact give rise to the desired map.

To put that clearly, we need some notations.

Consider the character Φ: $G_M = \mathrm{Gal}(\bar{\mathbb{Q}}/M) \longrightarrow \Lambda_L^X$ defined by as the Galois avatar of the character η: $G_\infty \longrightarrow \Lambda_L^X$,i.e. the composition of the restriction $G_M \longrightarrow \mathrm{Gal}(M(\mathfrak{f}p^\infty)/M)$ followed by the inverse reciprocity law $\mathrm{Gal}(M(\mathfrak{f}p^\infty)/M) \simeq G_\infty$ and finally by η.

Note that if $\mathfrak{M}_L$ is the maximal ideal of Λ_L, $\Phi \bmod.\mathfrak{M}_L = \hat{\lambda} \bmod.\mathfrak{P}$ $\mathfrak{P}$ being the maximal ideal in $\mathcal{O}_L$. In particular, $\Phi \not\equiv \Phi o[\rho] \bmod.\mathfrak{M}_L$ because $\hat{\lambda} \not\equiv \hat{\lambda} o[\rho] \bmod.\mathfrak{P}$ ($\hat{\lambda}$ is unramified at p^ρ whereas $\hat{\lambda} o[\rho]$ is).

Let $R_1(\Phi)$ the R_1-free module of rank one over which G_M acts via Φ; let $V = \mathrm{Ind}_{\mathbb{Q}}^{M} R_1(\Phi)$ the $G_{\mathbb{Q}}$-module induced from $R_1(\Phi)$, i.e.

$V = \mathcal{O}_L[G_{\mathbb{Q}}] \otimes_{\mathcal{O}_L[G_M]} R_1(\Phi)$; finally, let V' be the contragredient representation.

Proposition 5.8: (i) There is an isomorphism R_1- and $G_{\mathbb{Q}}$-linear:

$$A^* \simeq V'$$

in particular, the G_M-module A splits into the sum of two G_M-modules $A = X \oplus Y$; G_M acting on X via Φ and on Y via $\Phi o[\rho]$, and the Pontryagin dual of X and Y is isomorphic to $C_0(\mathcal{X})$ as R_1-module.

(ii) The module B^* contains no non-zero G_M-eigenvector.

Proof: (i) We first show that $A^* \otimes \mathcal{X} \simeq V' \otimes \mathcal{X}$ by equalizing the characteristic polynomials of the two representations. By Igusa's theorem [14], $J_1(Np^r)$ has good reduction over $\mathbb{Q}$ at any prime $\ell \nmid Np$, so A^* is unramified at such primes. Let $Frob_\ell$ act on A^*; thanks to the definition of Galois action on the jacobian, we see that $Frob_{\ell,Pic}$ is killed by $X^2 - T(\ell)X + \ell\langle\ell\rangle_2$ on $J_1(Np^r)[p^\infty]$; we see that the image of this polynomial by the character χ, coincides with $(X-\eta(\mathcal{L}))\cdot(X-\eta(\mathcal{L}^\rho))$ if ℓ splits in $\mathcal{L}\cdot\mathcal{L}^\rho$ in M and with $X^2 + \eta((\ell))$ if ℓ is inert. By Cebotarev's density theorem, we obtain the equality of the characteristic polynomials. So, this proves $A^* \otimes \mathcal{X} \simeq V' \otimes \mathcal{X}$ as $G_{\mathbb{Q}}$-modules. Furthermore, since $\Phi \not\equiv \Phi o[\rho] \bmod \mathfrak{M}_L$, we see that A^* is the sum of two submodules (necessarily free of rank one since R_1 is local): $A^* = \mathrm{Ker}(\sigma - \Phi(\sigma)) \oplus \mathrm{Ker}(\sigma - \Phi o[\rho](\sigma))$ for some $\sigma \in G_M$ such that $\Phi(\sigma) \not\equiv \Phi o[\rho](\sigma) \bmod \mathfrak{M}_L$; after tensoring with $\mathcal{X}$, they coincide with the stable lines of $A^* \otimes \mathcal{X}$, hence they are stable by G_M with the predicted action and they are interchanged by

the complex conjugation: $A^* \simeq V'$.

Now, let us prove (ii).

Suppose, by absurdity, that $x^* \in B^*$ is a non zero G_M-eigenvector. We may suppose further that $x^* \notin \omega_{2,1}.B^*$ because B^* has no Λ_L-torsion. Let x_1^* be its reduction. The algebra $F = (R_2/\omega_{2,1}.R_2)\otimes L$ is semi-simple because it is ordinary and the non-p-part of its Nebentypus is primitive, so it belongs to ordinary-primitive components. Then, $B_1^* = F\oplus F$, and $B_1^* \simeq \mathrm{Hom}(\mathrm{Ta}(B_1), \mathcal{O}_L)$ by an isomorphism α which is R-and $G_{\mathbb{Q}}$-linear. On one hand, we may decompose $B_1^*\otimes L$ as $\oplus\, e_{L'}.(B_1^*\otimes L)$ where $e_{L'}$ runs over the idempotents of $F = \prod L'$, so that for one such component, we must have $e_{L'}.x_1^* \neq 0$; on the other hand, the image by α of this element has a non-trivial kernel which is a L'-line in the plane $L'\otimes \mathrm{Ta}(B_1)$. This would mean by the theorem 4.5 of [28] that the modular form corresponding to the character $h_2(\Gamma_1(Np), L) \to L'$ given by $e_{L'}$ could be written as $\theta(\varphi)$ for some Grössencharacter φ of M. This is impossible: in fact, φ should have type (1,0) and conductor $f'p$ so that $Nf'.p = Np$, so it should differ from μ previously defined only by a Dirichlet character: $\varphi = \xi.\mu$ and by reducing modulo $\mathfrak{P}$ in the common field of values of those characters, we would find $\xi \equiv 1$ mod.$\mathfrak{P}$, i.e. ξ is a character of p-power order of the ray-class group modulo $ff'p$; by the hypothesis $p \nmid N\varphi(N)$, ξ is a character of the class group, hence of G_1, i.e. $\xi = \varepsilon'$ but $\varphi = \mu\varepsilon'$ furnishes a component of R_1, not of R_2: contradiction.

The next step is to form the R_2-and G_M-module $B^{(1)} = B/Y$

Let $X^{(1)}$ be the image of X in $B^{(1)}$. We define $Y^{(1)}$ by the short

exact sequence:

(5.6) $\quad 0 \to X^{(1)} \to B^{(1)}[c_2] \xrightarrow{\pi} Y^{(1)} \to 0$

Lemma 5.9: (i) The sequence of R_2-modules (5.6) is split.

(ii) The action of G_M on $X^{(1)}$ is given by Φ and on $Y^{(1)}$ by $\Phi o[\rho]$.

Proof: By dualizing the defining sequence of $B^{(1)}$, we find its structure over R_2:

$$B^{(1)*} = R_2 \oplus c_2 .$$

More precisely, by lifting the basis of $B[c_2]^*$ adapted to the sum $X^* \oplus Y^*$, we obtain by dualizing (5.6) the sequence:

(5.7) $\quad 0 \to c_2/c_2^2 \to R_2/c_2 \oplus c_2/c_2^2 \to R_2/c_2 \to 0$

where the maps are just the obvious inclusion of the second factor and the projection on the first factor. Since the projection of B to $B^{(1)}$ is G_M-linear by definition, we know that the action of G_M on $X^{(1)}$ is given by Φ. For $Y^{(1)}$ we use Eichler-Shimura relations: for $\sigma \in G_M$ acting on $B^*/c_2.B^*$, the matrix adapted to the decomposition (5.7) takes the form: $\sigma = \begin{pmatrix} a & * \\ & \Phi^{-1}(\sigma) \end{pmatrix}$ and is killed by the reciprocical polynomial of $X^2 - T(\ell)X + \ell\langle\ell\rangle_2 = (X-\Phi(\sigma)).(X-\Phi o[\rho](\sigma))$ in R_2/c_2 (once chosen a prime ℓ approximating σ ...). Hence, $a \equiv \Phi o[\rho](\sigma) \bmod c_2$.

Now, we are able to define the map of our dreams:

Fix arbitrarily a splitting over R_2 of the exact sequence (5.6)

Depending on this splitting, we have a map:

$$a: G_M \to \mathrm{Hom}_{R_2}(Y^{(1)}, X^{(1)}),\ \sigma \to \mathrm{pr}_{X^{(1)}} o\ \sigma_{\mathrm{Pic}}|_{Y^{(1)}}$$

Remark: This is the analogous of the coefficient in the upper right corner of the matricial representation defined by Hida in

theo.0.1 of [9].

It is easy to deduce from lemma 5.10 that $\mathrm{Hom}_{R_2}(Y^{(1)},X^{(1)})$ is R_2-isomorphic to $c_2/{c_2}^2$. It is the module of differentials attached to $\chi:R \to R_1$ defined by Hida in §1 of [13]. If R_1 was etale over Λ_L (which is unfortunately not the case), this module would have a more intrinsic definition which explains better its appellation:

$$C_1(\chi) = \Omega_{R/\Lambda_L} \otimes_\chi R_1$$

The coincidence of these two definitions for R_1/Λ_L etale is seen by using the second fundamental sequence for Kähler differentials (cf.[19] chap.10 Theo.58):

$$0 \to c_2/{c_2}^2 \to \Omega_{R/\Lambda_L} \otimes_\chi R_1 \to \Omega_{R_1/\Lambda_L} = 0$$

In any case, we will see later (§8) that, though this module of differential may not be isomorphic to $C_0(\mathcal{X})$, it is closely connected to it.

In the next paragraph, we are going to study the properties that a enjoys.

6. The properties of the map a.

The first property of a is its cocycle-like behaviour:

Lemma 6.1 : For all σ, σ' in G_M , we have:

(6.1) $\quad a(\sigma.\sigma') = a(\sigma).\Phi o[\rho](\sigma') + \Phi(\sigma).a(\sigma')$.

Hence, it defines by restriction to $G_{\tilde{K}_\infty} = Gal(\bar{\mathbb{Q}}/\tilde{K}_\infty)$ a group homomorphism we shall denote a_∞ in the following, from the Galois group of the maximal abelian p-extension of $\tilde{K}_\infty$ to the module of differentials $C_1(\chi) = c_2/{c_2}^2$. Furthermore, it carries the action by conjugation of $Gal(\tilde{K}_\infty/M)$ over $\mathcal{G}_{\tilde{K}_\infty}$ to the action via the "anticyclotomic" character $\Phi/\Phi o[\rho]$:

$$(6.2) \qquad a_\infty(\sigma^\tau) = \Phi(\tau)/\Phi o[\rho](\tau).a_\infty(\sigma).$$

In particular, in the decomposition $\tilde{\Gamma} = \Gamma^+ \times \Gamma^-$, the action of Γ^+ on $a(\mathcal{G}_{\tilde{K}_\infty})$ is trivial, and the action of the chosen generator w^- of W^- is multiplication by $\hat{\lambda}_0(w)$ where $w = \sqrt[p^d]{u} \in W$ and $u = 1+Np$. Moreover, the action of the non-p-part of $Gal(\tilde{K}/M)$ by conjugation factorises through Δ' (the non-p-part of $\Delta = Gal(K/M)$ and is given by κ defined in (4.1).

Remark: The penultimate assertion explains why we chose w^- so. Note also that a is not exactly a 1-cocycle of G_M but rather behaves exactly like the coefficient in the upper-right corner of the triangular matrix $\begin{pmatrix} \Phi(\sigma) & a(\sigma) \\ & \Phi(\sigma^\rho) \end{pmatrix}$; we could write this matrix if $B[c_2]$ was cofree over the ring R_2/c_2 but this is not so. Maps satisfying (6.1) are called binding-functions and studied in [4] §73.17.

Proof: In fact, the proof is very easy just by looking at the definition of a and we skip it.

The difficulty in studying a_∞ lies first in the ramification conditions assuring us it will factor through the maximal unramified outside S, p-abelian extension of $\tilde{K}_\infty$. This will require algebro-geometric considerations. That's why we will rather deal with $\underline{R}$ than with R (recall that $\underline{R}$ is the local component of $h^{ord}(Np^\infty,\mathbb{Z}_p)$ through which χ factorises). We may define $\underline{c}_1$ and $\underline{c}_2$, $\underline{R}_1$ and $\underline{R}_2$, $\underline{A}$ and $\underline{B}$, $\underline{B}^{(1)}$ $\underline{X}$, $\underline{X}^{(1)}$ $\underline{Y}$, $\underline{Y}^{(1)}$ in the same way as above, but they are true (ind-) p-divisible groups, resp. (ind-)finite group schemes and the one we have to study are just a part of their scalar extension from $\mathbb{Z}_p$ to $\mathcal{O}_L$. Hence it is enough to study those underlined modules. However, to lighten the notations, we will omit this underline.

Proposition 6.3: The map a is unramified outside p over $\tilde{K}$.

Remark: This means that it is unnecessary to restrict a to $\mathcal{G}_{\tilde{K}_\infty}$ to obtain the unramifiedness outside p : restriction to $G_{\tilde{K}}$ is enough ; whereas for the unramifiedness above p^ρ this will be unavoidable.

Proof: We see easily that

$$\begin{cases} B[c_2] = \varinjlim_r B_r[c_2] \\ B^{(1)}[c_2] = \varinjlim_r B_r^{(1)}[c_2] \end{cases}$$

with R_2-and G_M-linear transition maps. Now, Igusa's theorem [14] shows that $J_1(Np^r)$ has good reduction over $\mathbb{Q}$ at any prime $\ell \nmid Np$. So, the inertia $I_\ell \cap G_M$ acts trivially on B_r and also on

$B_r^{(1)}$ which is a p-divisible group M-isogenous to B.

For $\ell|N$, we use essentially the hypotheses $(f,f^\rho)=1$ and $p\nmid N\varphi(N)$ which assure us that the ℓ-part of the Nebentypus of the new forms occuring in the component R is primitive. Hence, a theorem of Langlands(Theo.7.1 and 7.4 of [18]) shows that B (and $B^{(1)}$) have good reduction at ℓ over $M(\zeta_{N_\ell})$; N_ℓ being the ℓ-part of N. Since this field is contained in $\tilde{K}$, we conclude that $I_\ell \cap G_{\tilde{K}}$ acts trivially on $B^{(1)}$ and hence that a is unramified at ℓ over $\tilde{K}$.

Now, we will prove unramifiedness above S over $\tilde{K}_\infty$. We need a lemma for that.

Let v be a place of $\tilde{K}_\infty$ above p^ρ. To stick better to the situation, we will consider instead of $\mathbb{Q}_p(\zeta_{p^r})$ and its ring of integers $\mathcal{O}_r$ as in (5.6), the completion $\mathfrak{K}_r$ of $\tilde{K}_r = M(p^r Nf)$ at v and its ring of integers $\mathfrak{O}_r$ (where as before $M(\mathfrak{a})$ stands for the ray class field of M of conductor $\mathfrak{a}$). Since $\mathfrak{O}_r$ is unramified over $\mathcal{O}_r$, this is an innocent base change and in particular the abelian scheme $A_{r/\mathfrak{O}_r}$ is only base change of $A_{r/\mathcal{O}_r}$ (*idem* for the schematic closure of $J_r(R)$ over $\mathfrak{O}_r$ and its connected-etale unscrewing (5.6)). We denote by B_r, $B_r^{(1)}$, X_r, Y_r, $X_r^{(1)}$ and $Y_r^{(1)}$ the $\omega_{2,r}$-torsion points of the corresponding previously defined objects. We consider the schematic closure of all of them over $\mathfrak{O}_r$. We hence have:

$$(6.3) \qquad 0 \to C_{r/\mathfrak{O}_r} \to B_r[c_2]_{/\mathfrak{O}_r} \xrightarrow{j} E_{r/\mathfrak{O}_r} \to 0$$

and similarly:

$$(6.4) \qquad 0 \longrightarrow C^{(1)}_{r/\Omega_r} \longrightarrow B^{(1)}_r[c_2]_{/\Omega_r} \xrightarrow{j^{(1)}} E^{(1)}_{r/\Omega_r} \longrightarrow 0$$

We omit the indexes Ω_r when we mean we take the geometric points of these sequences. We set X_r^- and Y_r^- for the schematic closures in $B_r[c_2]_{/\Omega_r}$ of X_r and Y_r . Let finally $D_{r,v}$ resp. D_v be the decomposition group of v in $G_{\tilde{K}_r}$ resp. in $G_{\tilde{K}_\infty}$.

Lemma 6.4: We have $Y_r = C_r$ and $X_r \overset{j}{\simeq} E_r$ so that X_r^- is etale and Y_r^- is connected.

Proof: see lemma 4.10 in [35] where this result is deduced from Theo.5.3.

From this lemma we may draw the proposition of unramification:

Proposition 6.5:The sequence (6.4) of $D_{r,v}$-modules splits for any r>0. In fact, $B^{(1)}_r[c_2] = C^{(1)}_r \oplus X^{(1)}_r$, $X^{(1)}_r \overset{j^{(1)}}{\simeq} E^{(1)}_r$, These splittings are compatible with the transition maps and by setting $C^{(1)} = \varinjlim_r C^{(1)}_r$, we have a D_v- linear splitting:

$$B^{(1)}[c_2] = C^{(1)} \oplus X^{(1)},$$

furthermore, the restriction of π to $C^{(1)}$ induces an isomorphism of D_v-modules to $Y^{(1)}$.

Recall that π is the projection from $B^{(1)}[c_2]$ to $Y^{(1)}$ defined in (5.6).

Corollary 6.6: At the prime v above p^ρ in $\tilde{K}_\infty$ not only a_∞ is unramified, but it is even totally split i.e. $a_\infty(D_v)=0$.

Proof: See Prop.4.11 in [35] where this is carefully proven. The corollary follows immediately.

An important remark is in order at this stage:

The generic fiber $C_{r/\mathfrak{R}_r}$ of the connected component of $B_1^*[c_2]$ descends canonically to the p^ρ-adic completion of M; in addition the inclusions $C_r^{(1)} \subset C_r^{(1)}$ are also defined over this field, so that the splitting:

$$B^{(1)}[c_2] = C^{(1)} \oplus X^{(1)}$$

is indeed stable under the decomposition group at p^ρ over M, say D. [This is easy : $B_r^{(1)}[c_2]$ is a G_M-module, so by universal property of the connected component, there exists for all σ in D a canonical isomorphism over $\mathfrak{R}_r$: $C_r^{(1)} \simeq C_r^{(1)\sigma}$ and descent conditions are obviously satisfied.]

This concludes the study of the ramification properties of a:

Proposition 6.7: The group homomorphism a_∞:

$$a_\infty : \mathcal{G}_{\tilde{K}_\infty} \longrightarrow C_1(\chi)$$

factorises through the Galois group $\mathfrak{X}$ of the maximal unramified outside S and totally splitted above S^ρ , p-abelian extension of $\tilde{K}_\infty$.

In fact, let X_∞^S be the Galois group of the maximal, unramified outside S, p-abelian extension of K_∞^- (the anticyclotomic $\mathbb{Z}_p$-extension of K) and let κ be the character of Δ=Gal(K/M) defined in (4.1), then a_∞ factorises naturally through the κ-part of X_∞^S :

$$(6.5) \qquad a_\infty \otimes Id_{\mathcal{O}_L} : X_\infty^S(\kappa) \longrightarrow C_1(\chi)$$

Furthermore if we endow $X_\infty^S(\kappa)$ with the twisted structure of I-module given by $(1+X)*x = (1+T).\hat{\lambda}_0(w).x$, then $a_\infty \otimes Id_{\mathcal{O}_L}$ becomes I-linear.

Proof: We only have to check that the natural restriction from

$\mathfrak{X}$ to X_∞^S induces an isomorphism on the κ-part of these groups. Let $\mathcal{N}$, resp. M_∞^S such that $\mathrm{Gal}(\mathcal{N}/K_\infty^-) = \mathfrak{X}$ and $\mathrm{Gal}(M_\infty^S/\tilde{K}_\infty) = X_\infty^S$. As $\tilde{K}_\infty/K_\infty^-$ is unramified, and the residual field of $\tilde{K}_\infty$ at $v|p^\rho$ has degree infinitely divisible by p, any p-extension of $\tilde{K}_\infty$ unramified at v is in fact totally split , so we can drop the condition above p^ρ and take care only of the unramifiedness outside S. Thus, we get $\tilde{K}_\infty \subset \mathcal{N} \subset M_\infty^S$; hence by restriction, we get an exact sequence:

$$X_\infty^S \dashrightarrow \mathfrak{X} \dashrightarrow \Gamma^+ \dashrightarrow 0$$

Since Δ' acts trivially on Γ^+, we obtain the surjectivity:

$$X_\infty^S(\kappa) \dashrightarrow \mathfrak{X}(\kappa)$$

Now, let κ_0 be the rational character of Δ' deduced from κ (it is no longer of degree one). We prove that the κ_0-part $M_\infty^S(\kappa_0)$ (maximal subextension of $M_\infty^S/\tilde{K}_\infty$ with action of $\mathbb{Z}_p[\Delta']$ on its Galois group through $e_{\kappa_0}.\mathbb{Z}_p[\Delta']$; e_{κ_0} = idempotent in $\mathbb{Z}_p[\Delta']$ corresponding to κ_0) is the compositum of $\tilde{K}_\infty$ and the κ_0-part of $\mathcal{N}$. This is obvious because the map $\mathrm{Gal}(M_\infty^S(\kappa_0)/K_\infty^-) \dashrightarrow \Gamma^+$ admits a section since the action of Δ' is trivial on Γ^+. This implies that $\mathcal{N}(\kappa_0)$ is the fixed part by Γ^+ of $M_\infty^S(\kappa_0)$, hence $M_\infty^S(\kappa_0) = \tilde{K}_\infty.\mathcal{N}(\kappa_0)$. This gives the isomorphism $X_\infty^S(\kappa_0) \simeq \mathfrak{X}(\kappa_0)$ and *a fortiori* $X_\infty^S(\kappa) \simeq \mathfrak{X}(\kappa)$.

The proposition 6.7 sums up the basic properties of a_∞. The last thing to prove about it is its surjectivity, thus establishing an important connection between the Iwasawa module and the module of differentials. This is the purpose of the next paragraph.

7. Surjectivity of a_∞.

We will be rather sketchy since this is detailed in §5 of [35]. We first define the Kummer-Wiles pairing attached the short exact sequence (4.6):

$$\langle , \rangle : X_\infty^S \times Y^{(1)} \to X^{(1)}, \quad \langle \sigma, P \rangle = \sigma.\tilde{P} - \tilde{P}$$

for any $\tilde{P}$ in $B^{(1)}[c_2]$ lifting $P \in Y^{(1)}$.

Let $Z = \{y \in Y^{(1)} \ ; \ \langle \sigma, y \rangle = 0, \ \forall \sigma \in X_\infty^S \}$; we see that $\mathrm{Im}(a_\infty \otimes \mathrm{Id}_{\mathbb{O}_L}) = \mathrm{Hom}_{R_2}(Y^{(1)}/Z, X^{(1)}) \subset \mathrm{Hom}_{R_2}(Y^{(1)}, X^{(1)})$. Hence, the surjectivity is equivalent to the nullity of Z. By absurdity, we suppose that $Z \neq 0$. There exists an ideal $\mathfrak{a}$ in R_2 such that $c_2^{\,2} \subset \mathfrak{a} \subset c_2$ and the Pontryagin dual sequence of

$$0 \to Z \to Y^{(1)} \to Y^{(1)}/Z \to 0$$

is $$0 \to \mathfrak{a}/c_2^{\,2} \to c_2/c_2^{\,2} \to c_2/\mathfrak{a} \to 0$$

Thus, the hypothesis $Z \neq 0$ is equivalent to $\mathfrak{a} \neq c_2$.

Now, we use the remark following prop.6.7 and fix some prime w in $\bar{\mathbb{Q}}$ above p^ρ; let D_w be th decomposition group at w in G_M. There is a R_2- and D_w-stable decomposition:

$$(7.2) \qquad B^{(1)}[c_2] = C_w^{(1)} \oplus X^{(1)}$$

and the projection π of (4.6) induces an isomorphism: $C_w^{(1)} \simeq Y^{(1)}$. Since p^ρ is almost inert in K_∞^-, we see that the restriction $G_M \to \mathrm{Gal}(K_\infty^-/M)$ maps D_w onto a finite index subgroup. By assuming (7.1), one constructs thanks to (7.2) an R_2 and G_M-submodule Z' in $B^{(1)}[c_2]$ on which G_M acts via $\Phi_0[\rho]$.

Let Y' its inverse image in B. Define $X^{(2)} = B[\mathfrak{a}]/Y'$.

The Pontryagin duals of Y' and $X^{(2)}$ are isomorphic to $R_2/\mathfrak{a}$. So we get a Galois representation of G_M on $B[\mathfrak{a}]^*$:

(7.3) $\qquad R: G_M \to GL_2(R_2/\mathfrak{a})$

which is upper triangular and such that $R(\sigma)= \begin{pmatrix} \alpha(\sigma) & \beta(\sigma) \\ 0 & \delta(\sigma) \end{pmatrix}$ with

$$\begin{cases} \alpha(\sigma) \equiv \Phi^{-1}(\sigma)_1 \bmod. c_2 \\ \delta(\sigma) \equiv \Phi \circ [\rho]^{-1}(\sigma) \bmod. c_2 \end{cases}$$

and, with some work, one proves that $\alpha=\Phi^{-1}$ and $\delta=\Phi\circ[\rho]^{-1}$.

From the existence of this representation, by using Eichler-Shimura relations, one deduces that the projections of Hecke operators $T(\ell)$(for all prime ℓ) in R_2 are congruent mod.$\mathfrak{a}$ to :

$$\begin{cases} \eta(\mathfrak{L})+\eta(\mathfrak{L}^{\rho}) & \text{if } \ell \nmid Np \text{ and splits in M} \\ 0 & \text{if } \ell \text{ is inert in M} \\ \eta(\mathfrak{L}) & \text{if } \ell \mid N \ . \end{cases}$$

This is an absurdity, because by the very definition of c_2 , this implies that $\mathfrak{a} \subset c_2$. Contradiction.

Hence we have proved the surjectivity.

To conclude the proof of Theo.4.3, it remains to give the link between the characteristic power series of $C_0(\mathfrak{X})$ and $C_1(\chi)$. This is the topic of the two next paragraphs.

8. An exact sequence for Congruence Module and Module of Differentials.

In this paragraph, we shortly recall the behaviour of the congruence module and the module of differentials with respect to the composition of characters (under suitable hypotheses, which we will check in our case). The reference for that, and some applications to the interpolation of special values of L-function associated with cusp forms is [40].

Let A be a complete local noetherian domain in characteristic zero with quotient field F; R and S are finite and flat A-algebras, and we are given two surjective characters $\lambda: R \to S$ and $\mu: S \to A$; we set $\nu=\mu\circ\lambda$. We suppose that μ, λ, ν (in this order) induce the following splittings:

$S\otimes_A F = F\oplus Y$, $R\otimes_A F = (S\otimes F)\oplus Z$, $R\otimes_A F = F\oplus X$ (of course, $X = Y\oplus Z$). We denote by S_Y, R_Z and R_X the images of S, R and R in Y, Z and X respectively.

Note that μ, λ, ν endow respectively A, S, A with a structure of S, R, R-module.

Then, the exact sequences we need are the following

Theorem 8.1: There is a canonical sequence of A-modules:

(8.1) $\mathrm{Tor}_1^R(\mathrm{Ker}\mu, A) \to C_1(\lambda, S)\otimes_S A \to C_1(\nu, A) \to C_1(\mu, A) \to 0.$

If $\mathrm{Hom}(S,A)\simeq S$ and $\mathrm{Hom}(R,A)\simeq R$ as R-modules, then there is also a short exact sequence for the congruence modules:

(8.2) $\quad 0 \to C_0(\mu,A) \to C_0(\nu,A) \to C_0(\lambda,S)\otimes_S A \to 0.$

[This is th.6.6 of [40]].

Proof: Since $\nu = \mu o \lambda$, λ induces a short exact sequence of R-modules:

(8.3) $\quad 0 \to \mathrm{Ker}\ \lambda \to \mathrm{Ker}\ \nu \to \mathrm{Ker}\ \mu \to \mathrm{Coker}\ \lambda = 0$

Recall that:

$$C_1(\mu,A) = (\mathrm{Ker}\ \mu)\otimes_S A = (\mathrm{Ker}\ \mu)\otimes_R A,$$

$$C_1(\nu,A) = (\mathrm{Ker}\ \nu)\otimes_R A$$

$$C_1(\lambda,S) = (\mathrm{Ker}\ \lambda)\otimes_R S$$

So, the exact sequence (8.1) comes out of (8.3) tensored with A over R.

Now, we suppose the assumptions on S and R. We consider again the short exact sequence (8.3).

We want to dualize it (i.e. apply functor $\mathrm{Hom}_A(-,A)$). For that, we first remark that Ker ν is A-free ($R \xrightarrow{\nu} A$ splits) and similarly, thanks to the freeness of S over A, we see that Ker μ and Ker λ are free. Furthermore, because of the A-freeness of S and the existence of an R-linear isomorphism $\mathrm{Hom}_A(R,A) \simeq R$, we see easily that $\mathrm{Hom}_A(\mathrm{Ker}\lambda,A) \simeq R_Z$ and $\mathrm{Hom}_A(\mathrm{Ker}\nu,A) \simeq R_X$ as R-modules. Similarly, $S \simeq \mathrm{Hom}_A(S,A)$ implies $\mathrm{Hom}_A(\mathrm{Ker}\mu,A) \simeq S_Y$. So, finally, we obtain an R-linear exact sequence:

(8.4) $\quad 0 \to S_Y \to R_X \to R_Z \to 0.$

We tensor it with A over R, using that:

$$C_0(\mu,A) = S_Y\otimes_S A = S_Y\otimes_R A,\ C_0(\nu,A) = R_X\otimes_R A,\ C_0(\lambda,S) = R_Z\otimes_R S$$

This yields:

$$\mathrm{Tor}_1^R(R_Z,A) \to C_0(\mu,A) \to C_0(\nu,A) \to C_0(\lambda,S)\otimes_S A \to 0.$$

The vanishing of the $\mathrm{Tor}_1^R(R_Z,A)$ comes from the following remark. We may present the R-module R_Z by: $0 \to R\cap S \to R \to R_Z \to 0$, where the intersection $R\cap S$ is taken in $S\oplus R_Z$. Now, $R\cap S$ is free of rank one over S because $\mathrm{Hom}_A(R,A) \simeq R$ induces an isomorphism $\mathrm{Hom}_A(R\cap S,A) \simeq S$ and we may dualize again because $R\cap S$ is A-free.

Hence, we get the R-linear exact sequence:

$$0 \to S \to R \to R_Z \to 0$$

We tensor it with A over R to obtain:

$$\mathrm{Tor}_1^R(R,A) \to \mathrm{Tor}_1^R(R_Z,A) \to S\otimes_R A \xrightarrow{\alpha} R\otimes_R A \to R_Z\otimes_R A \to 0,$$

we have $\mathrm{Tor}_1^R(R,A) = 0$ and $S\otimes_R A \simeq R\otimes_R A \simeq A$. Since $R_Z\otimes_R A$ is nothing but $C_0(\lambda,S)\otimes_S A$, it is A-torsion, so that the scalar in A giving α is non-zero, that is, α is injective and $\mathrm{Tor}_1^R(R_Z,A)=0$.

Now, we apply this theorem to our situation. We take $A = I$, $R = R\otimes_{\Lambda_L} I$, $S = I\otimes_{\Lambda_L} I$, $\lambda = \chi\otimes \mathrm{Id}_I$, $\mu = m$ (i.e. the multiplication $I\otimes I \to I$), $\nu = \mu\circ\lambda$. We have $C_0(\lambda,S) = C_0(\chi)\otimes I$ and $C_1(\lambda,S) = C_1(\chi)\otimes I$. Let us compute $C_0(m,I)$ and $C_1(m,I)$.

Lemma 8.2: $C_0(m,I) = C_1(m,I) = p^d I$.

Proof: $I\otimes I = I[Y]/(Y^{p^d} - (1+X)^{p^d}) \simeq I[z]/(z^{p^d}-1)$ as I algebras. because $1+X$ is invertible in $I = \mathcal{O}_L[[X]]$. Moreover, the morphism m: $I[z]/(z^{p^d}-1) \to I$ sends z to 1. Hence, we are in the situation of the group algebra of a cyclic group of order p^d and we apply lemma 1.9 of [13] to conclude.

From the theorem 8.1, we get I-linear exact sequences:

$$(8.1^{bis}) \quad \mathrm{Tor}_1^{R\otimes I}(\mathrm{Ker}\ m, I) \to C_1(\chi) \to C_1(\nu,I) \to I/p^d I \to 0$$

and (8.2^{bis}) $0 \to I/p^d I \to C_0(\nu, I) \to C_0(\chi) \to 0$

We get from these exact sequences some informations about the characteristic power series in I of the modules occuring in them. From (8.2^{bis}), we deduce that the characteristic power series $\mathbb{F}_\nu$ of $C_0(\nu, I)$ is $p^d H_{(\lambda, \iota_p)}(X)$ [where $H_{(\lambda, \iota_p)}(X)$ is a generator in I of $c_1 = R \cap (I \oplus \{0\})$ as defined in 4.2]. From (8.1^{bis}), we deduce that the characteristic power series $\mathbb{F}'_\nu$ of $C_1(\nu, I)$ divides p^dx(char. pow. ser.in I of $C_1(\chi)$). In the next paragraph, we will show that $\mathbb{F}_\nu$ divides $\mathbb{F}'_\nu$. This will complete the proof of th.4.3 because it implies that $H_{(\lambda, \iota_p)}(X)$ divides in I the characteristic power series in I of $C_1(\chi)$.

9. A link between the Fitting ideals of C_0 and C_1.

We use the concept of Fitting ideal rather than chracteristic power series because it behaves better with respect to base change of ring . Recall its definition.

Let R be a (noetherian) ring and M a R-module finitely presented and torsion. Take any presentation (ε, j):

$$R^a \xrightarrow{\varepsilon} R^b \xrightarrow{j} M \longrightarrow 0$$

The Fitting ideal of M is defined to be the ideal in R generated by the bxb minors of a matrix for ε. It doesn't depend on the choice of the presentation. For its basic properties, see [24] chap.3 and the appendix in [21]. Take R to be a P.I.D. ; then $M \simeq R/(d_1)x\ldots xR/(d_m)$, and the Fitting ideal of M is $(d_1\ldots d_m)$. Take R to be $R_0[[T]]$, for some discrete valuation ring R_0; then M is pseudo-isomorphic to $R/(d_1)x\ldots$ $\ldots xR/(d_m)$ for some well-defined d_i in R, and the Fitting ideal of M, F(M),admits the principal ideal $(d_1\ldots d_m)$ for its reflexive envelope (it means that the characteristic power series of M generates the intersection of all the localisations of F(M) at primes of height one).

We take R = I , the integral closure of Λ_L in $\mathcal{X}$. It is isomorphic to $\mathcal{O}_L[[X]]$ as we saw before. The modules we consider are $C_0(\nu, I)$ and $C_1(\nu, I)$ where $\nu = mo(\chi \otimes Id_I)$: $R \otimes_{\Lambda_L} I \longrightarrow I$ as defined in the previous paragraph.

To conclude the proof of Theo.4.2, we only have to check that the Fitting ideal $\mathcal{F}_1$ of $C_1(\nu,I)$ is contained in the Fitting ideal $\mathcal{F}_0$ of $C_0(\nu,I)$; this will be checked locally at each prime of height one in I (enough because $\mathcal{F}_0$ is principal). The general result yielding that inclusion is as follows :

Let D a complete discrete valuation ring, of quotient field $\mathcal{K}$, uniformizing parameter π, residual field k. Let $\mathcal{R}$ be finite and free algebra with a character $\nu : \mathcal{R} \to I$, inducing a generic splitting:

$$(8.1) \qquad \mathcal{R} \otimes \mathcal{K} \simeq \mathcal{K} \oplus \mathcal{B}$$

Let $\chi_1=\nu$ and χ_2 be the two projections, and $c_1 = \mathrm{Ker}\ \chi_2|_R$, $c_2 = \mathrm{Ker}\ \chi_1|_R$. Set as above $C_0 = I/\chi_2(c_1)$, $C_1 = c_2/c_2^2$, with Fitting ideals respectively F_0 and F_1.

Proposition 6.1: In the above situation, we have $F_1 \subset F_0$.

This result has been explained to me by M. Raynaud.

We apply it to the localisation in I at some prime P of height one of I, say $D=I_P$ which is a discrete valuation ring, and to the ring $\mathcal{R}=(R\otimes I)_P$ localisation at P of $R\otimes I$. Note that because I_P is a discrete valuation ring, R_P is free, and the datas of the proposition are furnished by localising at P the above datas. This gives for all such P the inclusion $\mathcal{F}_{0,P} \subset \mathcal{F}_{1,P}$ .Q.E.D.

The proof is divided in two parts. First, we establish even the equality of those ideals in the case where $\mathcal{R}$ is a complete intersection algebra. Then, for a general $\mathcal{R}$, we construct a complete intersection algebra $\mathcal{R}'$ finite and free over D with a character ν'; $\mathcal{R}' \to D$ admitting a generic splitting, and a

surjective morphism $\mathcal{R}' \to \mathcal{R}$ commuting with χ and χ' inducing isomorphism on the C_1's. This is enough because the F_0's can only decrease from $\mathcal{R}'$ to $\mathcal{R}$. We only detail here the first part. The second can be found in [35] §6.

Let $\mathcal{A}$ be the ring of polynomials in d variables over D.

Definition 6.2: We say that a sequence $(f_1,\ldots,f_d)$ of elements in $\mathcal{A}$ is relatively regular if for each i=1,...,d, the D-algebra $\mathcal{A}_i = \mathcal{A}/(f_1,\ldots,f_i)$ is flat over D and f_i doesn't divide zero in $\mathcal{A}_{i-1}$.

Definition 6.3 : We say that the algebra $\mathcal{R}$ is complete intersection over D if it admits a presentation

(8.3) $\quad 0 \to \mathcal{I} \to \mathcal{A} \to \mathcal{R} \to 0$

where the ideal $\mathcal{I}$ can be generated by a relatively regular sequence.

Suppose it is so. Take the second fundamental sequence for Kähler differentials ([19] Th ..58) for (8.3):

$$\mathcal{I}/\mathcal{I}^2 \to \Omega_{\mathcal{A}/D}\otimes_{\mathcal{A}} \mathcal{R} \to \Omega_{\mathcal{R}/D} \to 0;$$

thanks to the assumption, $\mathcal{I}/\mathcal{I}^2$ is free of rank d over $\mathcal{R}$, and the first map is injective. The D-module C_1 is isomorphic to $\Omega_{\mathcal{R}/D}\otimes_{\nu} D$ as noticed in 4 . We draw from that a free resolution of the finite length D-module C_1:

$$0 \to \mathcal{I}/\mathcal{I}^2 \otimes_{\mathcal{R},\nu} D \to \Omega_{\mathcal{A}/D}\otimes_{\mathcal{A}}\mathcal{R}\otimes_{\mathcal{R},\nu} D \to C_1 \to 0$$

Hence, F_1 is principal, generated by $\nu(\delta)$ where $\delta\in\mathcal{R}$ is the specialisation from $\mathcal{A}$ to $\mathcal{R}$ of the jacobian $\det(\partial f_i/\partial x_j)$. Let $\delta_1 = \chi_1(\delta)$ and $\delta_2 = \chi_2(\delta)$. Thanks to a remark of J. Tate explained in the appendix of [20], we know that $\mathrm{Hom}_D(\mathcal{R},D)$ is free over D and δ is a different for $\mathcal{R}$. That is, there is a basis $\{\lambda\}$ of

$\mathrm{Hom}_D(\mathcal{R},D)$ such that $\mathrm{Tr}_{\mathcal{R}/D} = \lambda.\delta$. Hence, to prove the equality of F_0 and F_1, it suffices to check:

$$\delta_1.D = \{ x_1 \in D \ ; \ (x_1,0) \in \mathcal{R} \}.$$

Since λ provides an autoduality of $\mathcal{R}$, this amounts to show that $x_1/\delta_1 \in D$ iff for any $y \in \mathcal{R}$, $\lambda((x_1,0).y) \in D$. We notice then that $(x_1,0) = (x_1/\delta_1,0).\delta$, so $\lambda((x_1,0).y) = \mathrm{Tr}_{\mathcal{R}/D}((x_1/\delta_1,0).y)$. Since $\mathrm{Tr}_{\mathcal{R}/D}$ induces the identity on the factor $\mathcal{K}$ of $\mathcal{R} \otimes \mathcal{K}$, the statement becomes obvious.

Bibliography

[1] M. Atiyah, I. Macdonald.- Introduction to Commutative Algebra. Addison-Wesley (1969).

[2] H. Carayol.- Sur les representations ℓ-adiques attachees aux formes modulaires de Hilbert. C. R. Acad. Sc. Paris, t. 296 Serie I, p. 629-632 (1985).

[3] J. Coates.- p-adic L function and Iwasawa theory, in Algebraic Number Fields, edited by A. Fröhlich, Academic Press 1977.

[4] C. Curtis, I. Reiner.- Representation Theory of Finite Groups and Associative Algebras. Interscience Publishers, John Wiley and Sons 1966.

[5] K. Doi, M. Ohta.- On some congruences between cusp forms on $\Gamma_0(N)$, in Modular Forms in One Variable, Proceedings International Conference, University of Bonn, L.N.M.601, p. 91-105, Springer-Verlag 1977.

[6] K. Iwasawa.- Lectures on p-adic L Functions. Ann. of Math. Stud. 74, Princ. Univ. Press 1972.

[7] H. Hida.- Congruences of cusp forms and special values of their zeta functions. Inv. Math. 63, p. 225-261 (1981).

[8] H. Hida.- On congruence divisor of cusp forms as factors of the special values of their zeta functions. Inv. Math. 64, p. 221-262 (1981).

[9] H. Hida.- Kummer's criterion for the special values of Hecke L-functions of imaginary quadratic fields and congruences among cusp forms.Inv. Math. 66, p. 415-459 (1982).

[10] H. Hida.- Iwasawa module attached to congruences of cusp

forms. Ann. Scient. Ec. Norm. Sup. 4^{eme} serie t.19, 1986, p.231-273.

[11] H. Hida.- Galois representations into $GL_2(\mathbb{Z}_p[[X]])$ attached to ordinary cusp forms. Inv. Math. 85, p. 545-577 (1986).

[12] H. Hida.- A p-adic measure attached to the zeta-functions associated with two elliptic modular forms, I. Inv. Math. 79, p. 159-195 (1985).

[13] H. Hida.- Hecke algebras for GL_1 and GL_2. Sem. Th. N. Paris , 1985-86, p. 131-163.

[14] J. I. Igusa.- Kroneckerian model of fields of elliptic modular functions. Amer. J. Math. 81, p. 545-577 (1959).

[15] N. Katz.- Higher congruences between modular forms. Ann. of Math. vol. 101, p. 332-367 (1975).

[16] N. Katz, B. Mazur.- Arithmetic Moduli of Elliptic Curves. Ann. of Math. Studies, Number 108. P.U.P.

[17] S. Lang.- Cyclotomic Fields I. G.T.M. Springer-Verlag 1978.

[18] R. P. Langlands.- Automorphic Forms and ℓ-adic representations, in Proceedings International Summer School on Modular Functions of One Variable, II, Antwerp 1972, L.N.M. 349 . 361-500, Springer-Verlag 1973.

[19] H. Matsumura.- Commutative Algebra. Benjamin 1970.

[20] B. Mazur, L. Roberts.- Local Euler characteristics, Inv. Math. 9 , 1970, p. 201-234 .

[21] B. Mazur, A. Wiles.- Class fields of abelian extensions of $\mathbb{Q}$, Inv. Math. 76, 1984, p. 179-330.

[22] B. Mazur, A. Wiles.-On p-adic analytic families of Galois representations. Comp. Math. 59, p. 231-264 (1986).

[23] D. Mumford.- Geometric Invariant Theory. Ergebnisse des Mathematik und Ihrer Grenzgebiete 34. Springer-Verlag 1965.

[24] D. Northcott.- Finite Free Resolutions. Cambridge Tracts in Maths. 71, Camb. Univ. Press 1976.

[25] B. Perrin-Riou.- Arithmetique des Courbes Elliptiques et Theorie d'Iwasawa. Memoires de le S.M.F. n^o 17, Nouvelle Serie (1984).

[26] K. Ribet.- p-adic interpolation via Hilbert modular Forms. In Alg. Geometry, Proc. Symp. Pure Maths., vol. 29, Humboldt State Univ., Arcata, Cal. 1974, pp. 581-592. Amer. Math. Soc. 1975.

[27] K. Ribet.- A modular construction of unramified extensions of $\mathbb{Q}(\mu_p)$. Inv. Math. 34, p. 151-162 (1976).

[28] K. Ribet.- Galois representations attached to eigenforms with Nebentypus. In Modular Functions of One Variable V, L.N.M. 601, p. 17-52, Springer-Verlag 1977.

[29] K. Ribet.- Fonctions L p-adiques et Theorie d'Iwasawa, notes d'un cours a Orsay, redige par Ph. Satge. Publ. Math. d'Orsay 1979.

[30] J.-P. Serre.- Representations Lineaires des Groupes Finis. Hermann, 1967.

[31] J.-P. Serre, J. Tate.- Good reduction of abelian varieties, Ann. of Math. vol.88, p. 492-517 (1968).

[32] G. Shimura.- Introduction to the Arithmetic Theory of Automorphic Forms. Iwanami Shoten Publishers and Princeton

University Press, 1971.

[33] G. Shimura.- On elliptic curves with complex multiplication as factors of the jacobians of modular function fields, Nagoya Math. J. 43, p. 199-208 (1971).

[34] J. Tilouine.- Un sous-groupe p-divisible de la jacobienne de $X_1(Np^r)$ comme module sur l'algebre de Hecke, to appear in Bull. Soc. Math. France (1987).

[35] J. Tilouine.- Theorie d'Iwasawa classique et de l'algebre de Hecke ordinaire, to appear in Comp. Math.

[36] L. Washington.- Introduction to Cyclotomic Fields. G.T.M. Springer-Verlag 1982.

[37] A. Weil.- On a certain type of characters of the idele class group of an algebraic number field. In Proc. Symp. on Algebraic Number Theory, Tokyo-Nikko, p. 1-7, 1955.See also in Collected Papers II, [1955c].

[38] A. Wiles.- Modular curves and the class-group of $\mathbb{Q}(\mu_p)$. Inv. Math. 58, p. 1-35 (1980).

[39] H. Hida.- A p-adic measure attached to the zeta-functions associated with two elliptic modular forms, II, to appear in Ann. Inst. Fourier.

[40] H. Hida.- Module of congruence of Hecke algebras and L-functions associated with cusp forms, to appear in Amer. J. of Math.

Current address: J.Tilouine
Bat.425, Mathematique
faculte des Sciences d'Orsay
91405 ORSAY Cedex 05 FRANCE